(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
24 décembre 2003 (24.12.2003)

PCT

(10) Numéro de publication internationale
WO 03/107587 A1

(51) Classification internationale des brevets[7] : H04L 9/32, 9/08

(21) Numéro de la demande internationale :
PCT/FR03/01841

(22) Date de dépôt international : 17 juin 2003 (17.06.2003)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
02/07413 17 juin 2002 (17.06.2002) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **CRYPTOLOG** [FR/FR]; 16-18, rue Vulpian, F-75013 Paris (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **STERN, Julien** [FR/FR]; 191, rue St. Denis, F-75002 Paris (FR). **PORNIN, Thomas** [FR/FR]; 13, rue Mademoiselle, F-75015 Paris (FR).

(74) Mandataire : **ABELLO, Michel**; Cabinet Peuscet, 78, avenue Raymond Poincaré, F-75116 Paris (FR).

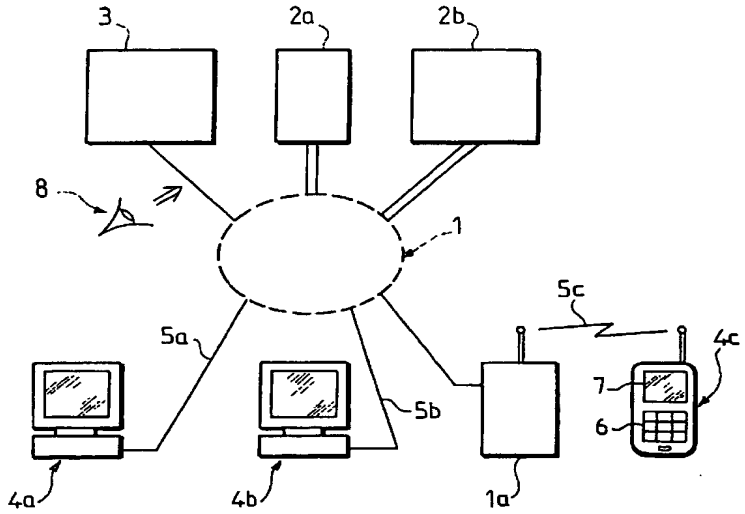
(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) États désignés *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet

[Suite sur la page suivante]

(54) Title: INTERFACE METHOD AND DEVICE FOR THE ON-LINE EXCHANGE OF CONTENTS DATA IN A SECURE MANNER

(54) Titre : PROCEDE ET DISPOSITIF D'INTERFACE POUR ECHANGER DE MANIERE PROTEGEE DES DONNEES DE CONTENU EN LIGNE



(57) Abstract: The invention relates to a method for the on-line exchange of contents data, comprising the following method steps: reception of a code entered by a user on an interface device (4a-c), transmission of a first read request from said interface device to a first server device (3), in which are stored the respective personal cryptographic data for a number of users encoded by using a respective authentic code for said user, reception of the encoded personal cryptographic data for said user in said interface device, decoding said personal cryptographic data by means of said entered code when the entered code corresponds to the authentic code for the user, use of said personal cryptographic data to secure an exchange of contents data between said interface device and at least one second server device (2a-b) and erasure of said entered code and said personal cryptographic data from said interface device.

[Suite sur la page suivante]

WO 03/107587 A1

européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— *avec rapport de recherche internationale*

— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(57) Abrégé : Procédé pour échanger des données de contenu en ligne, comportant les étapes consistant à: recevoir un code entré par un utilisateur dans un dispositif d'interface (4a-c), envoyer une première requête de lecteur depuis ledit dispositif d'interface à un premier dispositif serveur (3) dans lequel sont stockées des données personnelles cryptographiques respectives d'une pluralité d'utilisateurs, chiffrées au moyen d'un code authentique respectif dudit utilisateur, recevoir les données personnelles cryptographiques chiffrées dudit utilisateur dans ledit dispositif d'interface, déchiffrer lesdites données personnelles cryptographiques au moyen dudit code entré lorsque ledit code entré correspond audit code authentique de l'utilisateur, utiliser lesdites données personnelles cryptographiques pour protéger un échange de données de contenu entre ledit dispositif d'interface et au moins un deuxième dispositif serveur (2a-b), supprimer ledit code entré et lesdites données cryptographiques personnelles dudit dispositif d'interface.

PROCÉDÉ ET DISPOSITIF D'INTERFACE POUR ÉCHANGER DE MANIÈRE PROTÉGÉE DES DONNÉES DE CONTENU EN LIGNE

La présente invention concerne un procédé et un dispositif d'interface pour échanger de manière protégée des données de contenu en ligne.

Le développement des réseaux de transport de données permet de concevoir et d'utiliser de nombreux services accessibles en ligne, c'est-à-dire accessibles à distance via un réseau de transport de données. Des exemples de tels services sont le commerce électronique, la diffusion de programmes audio-visuels, le courrier électronique, les services de gestion bancaire et financière en ligne, l'accès aux banques de données et l'accès nomade à un bureau virtuel, entre autres. Ce type de service est généralement rendu accessible par le fournisseur du service au moyen d'un ou plusieurs serveur(s) de données relié(s) au réseau de transport de données. L'utilisation de tels services implique d'échanger des données de contenu, c'est-à-dire des données qui véhiculent le contenu du service, entre un dispositif d'interface d'utilisation et au moins un serveur du fournisseur du service, via le réseaux de transport de données.

Or ces données de contenu présentent généralement un caractère personnel ou réservé pour l'utilisateur et/ou pour le fournisseur du service. Pour empêcher tout tiers d'acquérir et d'utiliser des données de contenu qui ne lui sont pas destinées, il est donc nécessaire de protéger les échanges de données de contenu contre différents risques. Ces risques peuvent tenir notamment à l'existence d'incertitudes quant à l'identité de l'expéditeur ou du destinataire des données échangées et aux possibilités de détournement ou d'altération des données au cours de leur transport depuis l'expéditeur jusqu'au destinataire légitime. Il faut ici comprendre les termes de destinataire et d'expéditeur comme désignant des ordinateurs ou appareils similaires reliés à un réseau de transport de données ou les utilisateurs ou les exploitants de tels ordinateurs ou appareils.

On connaît différentes méthodes cryptographiques pour assurer une telle protection. Par exemple, les méthodes de signature électronique permettent à tout destinataire d'un message de vérifier l'identité de l'expéditeur et de vérifier que le contenu du message n'a pas

été altéré au cours de son transport. Les méthodes d'authentification permettent de vérifier l'identité du correspondant avec lequel l'échange de données est effectué. Les méthodes de chiffrement, symétriques ou asymétriques, permettent de mettre les données dans une forme inutilisable par tout tiers autre que leur destinataire légitime. Ces méthodes cryptographiques connues peuvent être combinées selon les besoins de chaque application.

La mise en œuvre de ces méthodes cryptographiques requiert l'emploi d'un dispositif d'interface capable d'effectuer des calculs complexes, c'est-à-dire d'un dispositif assimilable à un ordinateur au sens large du terme, comme une station de travail, un téléphone cellulaire, un assistant numérique personnel, un micro-ordinateur, un décodeur de télévision ou une carte à puce. Cette mise en oeuvre est généralement possible à l'aide d'une implantation logicielle de la méthode sur le dispositif d'interface, implantation logicielle qui peut être éventuellement publique.

Cependant, l'implantation logicielle ou matérielle de la méthode cryptographique, quelle qu'elle soit, n'est utilisable par une personne pour protéger des données de contenu que lorsque cette implantation est configurée au moyen de données cryptographiques personnelles, c'est-à-dire spécifiques à cette personne. Il existe des données cryptographiques personnelles qui sont à usage public, comme une clé publique permettant à tout tiers de vérifier les signatures électroniques émises par cette personne, et des données cryptographiques personnelles qui sont à usage privé, comme une clé privée permettant à la personne d'émettre sa signature propre. Il est impératif de conserver secrètes ces données cryptographiques personnelles, du moins celles qui sont à usage privé. En effet, si une personne autre que le propriétaire authentique des données cryptographiques personnelles prend possession de celles-ci, cette personne peut utiliser tous les services en ligne au nom du propriétaire authentique et sans être facilement démasquée.

On connaît plusieurs solutions pour conserver de telles données cryptographiques personnelles.

Une première solution consiste à utiliser des données cryptographiques personnelles qui sont intrinsèques à leur propriétaire et ne nécessitent donc pas de moyen de stockage matériel. Ce type de

données cryptographiques personnelles englobe les mots de passe mémorisés par leur propriétaire et les données biométriques, comme les empreintes digitales et les images rétiniennes.

L'inconvénient des données biométriques est de requérir l'emploi d'un lecteur spécifique dont le coût est élevé et dont l'emploi n'est pas très répandu. De plus, les données biométriques ont une configuration fixe qu'il n'est pas possible d'adapter à tous les formats utiles, par exemple pour leur emploi dans les méthodes standard d'authentification et de chiffrement tels que OpenPGP (acronyme de l'anglais : Open Pretty Good Privacy), S/MIME (acronyme de l'anglais : Secure Multipurpose Internet Mail Extensions), SSL (acronyme de l'anglais : Secure Socket Layer).

L'inconvénient des mots de passe est qu'ils imposent un compromis, pas toujours acceptable, entre sécurité et ergonomie. En effet, plus le mot de passe est court, plus sa mémorisation est aisée mais plus le chiffrement qui repose sur le mot de passe est aisé à casser par une recherche systématique, du fait du nombre réduit de combinaisons à essayer. Inversement, plus le mot de passe est long, plus le niveau de sécurité du chiffrement correspondant est élevé, mais plus la mémorisation devient difficile. Ecrire le mot de passe sur un aide-mémoire entraîne des risques de divulgation et un oubli du mot de passe par son propriétaire entraîne un risque de pertes des données qu'il a servi à chiffrer.

Une deuxième solution connue consiste à stocker les données cryptographiques personnelles localement sur l'appareil qui met en œuvre la méthode cryptographique dans laquelle lesdites données sont exploitées. Cette solution consiste par exemple à stocker ces données sur le disque dur d'un micro-ordinateur servant de dispositif d'interface d'utilisation des services en ligne ou dans la mémoire non volatile d'un téléphone cellulaire.

Les inconvénients de cette solution sont multiples : une personne ne peut échanger de manière protégée des données de contenu qu'en utilisant l'unique appareil sur lequel ses données cryptographiques personnelles sont stockées. Il n'est alors possible d'utiliser des services en ligne que depuis un lieu unique, à moins d'utiliser un appareil portatif et de l'emporter en tout lieu d'utilisation des services. De plus, les accès

à l'appareil doivent être contrôlés, pour empêcher l'accès d'une personne non autorisée aux données cryptographiques personnelles. L'appareil peut bien être placé dans une chambre forte ou un environnement protégé similaire dans certains cas, mais cette mesure n'est pas compatible avec tous les contextes d'utilisation des services en ligne, par exemple avec le contexte d'une utilisation nomade depuis un téléphone cellulaire. En outre, si l'appareil doit servir à plusieurs utilisateurs, il doit alors stocker les données cryptographiques personnelles de tous les utilisateurs potentiels, ce qui augmente le volume de stockage nécessaire. Enfin, les données cryptographiques personnelles peuvent être irrémédiablement perdues en cas de destruction, de disparition ou de panne de l'appareil.

La duplication des données cryptographiques personnelles sur plusieurs appareils ne résout pas tous ces problèmes. Au contraire, elle rend un contrôle des accès aux multiples appareils plus difficile à effectuer.

Dans le cas des ordinateurs de bureau, on connaît aussi une troisième solution combinant les deux solutions susmentionnées. Les données cryptographiques personnelles sont stockées localement sur l'ordinateur mettant en œuvre les méthodes cryptographiques dans lesquelles elles sont exploitées, mais ce stockage est réalisé sous une forme chiffrée symétriquement à l'aide d'une clé dérivée d'un mot de passe. Les standards PKCS#12 et OpenPGP décrivent cette troisième solution.

Un inconvénient de cette troisième solution connue réside dans le fait qu'un tiers ayant pris possession de l'appareil dispose de tous les moyens de tenter de se procurer les données cryptographiques personnelles en cassant leur chiffrement par des essais systématiques de mots de passe, ce qui constitue une attaque dite « par dictionnaire ».

Une quatrième solution connue consiste à stocker les données cryptographiques personnelles sur une carte à puce. Le document EP 1 150 506 A2 décrit un système utilisant cette solution pour une application de diffusion de données vidéo numériques.

Une carte à puce est facile à transporter et peut être blindée. Toutefois, la résistance du blindage dépend du coût et du format de la

carte à puce. Il est connu que celui des cartes à puce usuelles peut être percé avec succès avec un budget de l'ordre de 10^4 Euros.

Les inconvénients de cette quatrième solution sont également la nécessité d'emporter la carte à puce en tout lieu d'utilisation des services, la nécessité de disposer d'un lecteur compatible sur le lieu d'utilisation, les risques de perte des données cryptographiques personnelles en cas de destruction, de disparition ou de panne de la carte à puce, et les risques de pertes de données de contenu chiffrées qui s'ensuivent.

US-A-5 491 752 décrit un procédé pour récupérer une clé privée sur un serveur distant depuis une station de travail agissant au nom d'un utilisateur, dans lequel :

- l'utilisateur entre son mot de passe dans la station de travail ;
- la station de travail transforme le mot de passe en clé de chiffrement symétrique par application d'un algorithme de hachage ;
- la station de travail demande au serveur distant la clé privée de l'utilisateur, qui est stockée sur le serveur distant sous forme chiffrée au moyen de la clé symétrique dérivée du mot de passe ;
- le serveur distant envoie cette clé privée sous forme chiffrée à la station de travail, qui la déchiffre avec la clé symétrique.

Les risques présentés par une telle récupération sont les suivants :

- si le mot de passe est récupéré par un tiers, la sécurité du système est directement compromise ;
- si les clés privées chiffrées sont récupérées par un tiers, ce tiers pourra tenter ce qu'on appelle une attaque par dictionnaire hors-ligne, c'est-à-dire pourra essayer un grand nombre de mots de passe habituels (tous les mots existants dans toutes les langues par exemple) sans interaction avec le serveur.

On peut alors exiger une authentification de l'utilisateur afin que le serveur distant ne transmette des clés chiffrées qu'à l'utilisateur auquel elles appartiennent. Pour cela, US-A-5 491 752 propose d'authentifier l'utilisateur possédant le mot de passe avant de lui envoyer ses clés chiffrées. Les techniques proposées consistent essentiellement à envoyer la valeur de hachage du mot de passe au serveur afin de lui

prouver la connaissance du mot de passe. Cette valeur doit être envoyée chiffrée afin qu'elle ne puisse être lue que par le serveur distant.

Cette authentification de l'utilisateur pourrait se faire de manière plus ou moins complexe, mais elle nécessite dans tous les cas que des données de vérification soient initialement stockées sur le serveur distant. Il est en effet impossible d'identifier un utilisateur ex nihilo. Il convient de remarquer que, quelle que soit la méthode utilisée, le serveur distant peut effectuer une attaque par dictionnaire hors-ligne. Les seules données caractérisant un utilisateur sont son identifiant (a priori public) et son mot de passe. Le serveur distant peut donc essayer un grand nombre de mots de passe puisqu'il possède un accès direct aux données de vérification.

Il convient donc d'éviter que les clés privées chiffrées, les données de vérification ou toute autre information permettant une attaque par dictionnaire hors-ligne soit obtenue par un tiers autre que le serveur effectuant les vérifications.

Pour assurer la confidentialité de la valeur de hachage du mot de passe, cet art antérieur suppose que la clé de chiffrement publique du serveur est connue. En d'autres termes, il est supposé qu'il existe déjà un canal permettant de garantir que les données envoyées seront reçues par le serveur distant et par lui seul.

Cette hypothèse est relativement forte. Il serait donc souhaitable d'avoir un système permettant d'empêcher les attaques par dictionnaire hors-ligne même dans le cas où l'on ne dispose pas a priori d'un canal authentifié et confidentiel avec le serveur, notamment dans une configuration minimaliste où la seule information certaine connue des deux parties est le mot de passe de l'utilisateur ou un dérivé de celui-ci.

Il est souhaitable en particulier que si les communications de l'utilisateur s'effectuent avec un faux serveur, ce dernier n'apprenne aucune information sur le mot de passe.

L'invention a pour but de remédier à au moins certains des inconvénients susmentionnés, en fournissant un procédé et un dispositif d'interface pour échanger de données de contenu en ligne qui assure une bonne protection des données de contenu, qui soit facile à utiliser et accessible aussi largement que possible.

Pour cela, l'invention fournit un procédé pour échanger de manière protégée des données de contenu en ligne comportant les étapes consistant à :
recevoir un code entré par un utilisateur dans un dispositif d'interface relié à un premier dispositif serveur par au moins un réseau de transport de données,
envoyer une requête de lecture depuis ledit dispositif d'interface audit premier dispositif serveur dans lequel sont stockées des données personnelles cryptographiques respectives d'une pluralité d'utilisateurs, lesdites données personnelles cryptographiques de chaque utilisateur étant chiffrées au moyen d'un code authentique respectif dudit utilisateur,
recevoir les données personnelles cryptographiques chiffrées dudit utilisateur dans ledit dispositif d'interface,
déchiffrer lesdites données personnelles cryptographiques au moyen dudit code entré lorsque ledit code entré correspond audit code authentique de l'utilisateur,
caractérisé par le fait qu'il comporte les étapes consistant à :
utiliser lesdites données personnelles cryptographiques pour protéger un échange de données de contenu entre ledit dispositif d'interface et ledit au moins un deuxième dispositif serveur relié audit dispositif d'interface par au moins un réseau de transport de données,
supprimer ledit code entré et lesdites données cryptographiques personnelles dudit dispositif d'interface.

Au sens de l'invention, un dispositif serveur est un ordinateur ou appareil similaire relié à un réseau de transport de données et programmé pour mettre des ressources matérielles et/ou logicielles à disposition de plusieurs utilisateurs, via des dispositifs d'interface d'utilisation, encore appelés dispositifs clients, également reliés au réseau de transport de données.

Au sens de l'invention, un réseau de transport de données désigne tout moyen de liaison apte à transporter des données, que ce soit sous forme optique, radioélectrique ou électrique, et peut être constitué de fibres optiques, de câbles électriques, de câbles coaxiaux, de stations d'émission/réception radiofréquences ou hyperfréquences ou à infrarouge, de routeurs, de répétiteurs, et de toute combinaison de ces

éléments connus de l'homme du métier. Plusieurs réseaux présentant au moins un point de passage des uns aux autres constituent aussi un réseau de transport de données au sens de l'invention.

Le stockage des données personnelles des utilisateurs dans le premier dispositif serveur, incluant des données personnelles cryptographiques, permet de rendre ces données accessibles à distance depuis un dispositif d'interface relié au premier dispositif serveur. Les données personnelles cryptographiques de l'utilisateur sont de ce fait tenues à sa disposition sans nécessiter le transport d'un appareil mobile ou d'une carte à puce.

Les données personnelles cryptographiques sont stockées sur le premier dispositif serveur sous une forme chiffrée au moyen d'un code authentique connu seulement de leur utilisateur légitime, de sorte que leur confidentialité est préservée, y compris vis-à-vis du premier dispositif serveur.

Le code authentique et les données personnelles cryptographiques chiffrées ou déchiffrées ne sont conservées sur le dispositif d'interface que le temps d'une session, c'est-à-dire le temps nécessaire à leur utilisation, respectivement pour déchiffrer les données personnelles cryptographiques reçues depuis le premier serveur et pour protéger par une méthode cryptographique un échange de données de contenu entre le dispositif d'interface et le deuxième dispositif serveur, après quoi elles sont supprimées du dispositif d'interface. Ainsi, l'utilisateur n'a pas besoin de contrôler les accès au dispositif d'interface entre deux sessions, lequel peut par conséquent servir à une multitude d'utilisateurs, par exemple selon une règle de libre service.

De préférence, ledit dispositif d'interface et ledit premier dispositif serveur établissent un canal de communication confidentiel entre eux par mise en commun d'au moins une clé de chiffrement présentant une grande entropie par rapport audit code authentique de l'utilisateur, lesdites données personnelles cryptographiques chiffrées étant transmises audit dispositif d'interface par ledit canal de communication confidentiel. Ceci offre un premier niveau de protection contre les attaques par dictionnaire d'un tiers interceptant les communications entre le dispositif d'interface et le premier dispositif serveur. Pour cela, on peut utiliser un protocole d'échange de clé ou

Key-Exchange qui permet à deux parties ne possédant aucune donnée secrète commune préalable de calculer une telle données puis de s'en servir par exemple comme clé de chiffrement symétrique, nommée alors clé de session.

De préférence, au moins une donnée personnelle de vérification de code qui dérive dudit code authentique de l'utilisateur selon une fonction déterministe est stockée dans ledit premier dispositif serveur et ledit premier dispositif serveur authentifie explicitement ou implicitement ledit dispositif d'interface à l'aide de ladite donnée personnelle de vérification de code. L'authentification implicite du dispositif d'interface signifie que le premier dispositif serveur, sans avoir aucune garantie sur l'identité de son interlocuteur dans ce cas, est assuré que seul un dispositif d'interface possédant le code authentique pourra interpréter sa réponse.

La fonction déterministe peut être la fonction identité, auquel cas le premier dispositif serveur stocke le code authentique lui-même. Avantageusement, ladite fonction déterministe est une fonction non inversible résistante aux collisions, en particulier une fonction de hachage cryptographique.

Selon un mode de réalisation particulier de l'invention, ledit dispositif d'interface et ledit premier dispositif serveur réalisent simultanément la mise en commun de ladite au moins une clé de chiffrement et l'authentification explicite ou implicite dudit dispositif d'interface par ledit premier dispositif serveur en utilisant un protocole de type Password-Based-Key-Exchange (échange de clé basé sur un mot de passe) PBKE.

Au sens de l'invention, on désigne par protocole de type PBKE une famille de protocoles également connus sous le nom de Password Authenticated Key Agreement (PAKA). Ces protocoles vérifient au moins les conditions suivantes :

- les deux parties n'utilisent qu'un code de faible entropie au sens du nombre des réalisations possibles, par exemple un mot de passe ou son dérivé, comme donnée certaine commune,
- à partir de cette donnée commune, les deux parties établissent un canal de communication sûr, c'est-à-dire

fondé sur au moins une clé de plus grande entropie, sans permettre les attaques par dictionnaire hors lignes des tiers cherchant à se procurer cette donnée commune,

- au moins une des deux parties acquiert une preuve d'authenticité de l'autre partie, l'authenticité étant définie comme la connaissance de la donnée certaine commune. Cette preuve d'authenticité peut être explicite ou implicite. Une authentification implicite ne fournit pas immédiatement la garantie d'authenticité de l'autre partie ; mais elle garantie que la clé de grande entropie protégeant le canal de communication sûr qui est établi au cours du protocole ne peut être connue de l'autre partie que si cette dernière connaissait la donnée certaine commune préalablement à l'exécution du protocole.

L'organisme de normalisation IEEE propose une liste de tels protocoles dans le document P1363.2 : Standard Specifications for Password-Based Public-Key Cryptographic Techniques, Version 7, 20 décembre 2002, qui est incorporé par référence. Les protocoles de type PBKE comprennent une sous-famille de protocoles dénommée Encrypted Key Exchange (EKE). L'EKE est un concept général, théoriquement applicable à n'importe quel protocole d'échange de clé ; mais, pour le moment, la recherche en cryptographie n'a mis au point les détails techniques que dans le cas de Diffie-Hellman et de ses variantes sur d'autres groupes (comme par exemple sur des courbes elliptiques).

Un tel protocole apporte une protection de ladite au moins une clé de chiffrement contre l'interception par un tiers qui intercepterait toutes les communications entre le dispositif d'interface et le premier dispositif serveur sans connaître ledit code authentique ou ses dérivés. Ce mode de réalisation offre une sécurité élevée qui ne repose pas sur l'existence préalable d'un canal sécurisé vers le serveur distant, ni sur l'existence d'information permettant d'en créer un de manière immédiate. La sécurité de ce mode de réalisation avec échange de clé basé sur un mot de passe ne repose en effet sur aucune autre donnée certaine prédéfinie que le mot de passe ou code authentique de l'utilisateur ou ses dérivés déterministes.

De préférence, ledit protocole de type Password-Based-Key-Exchange inclut une seule communication dans chaque sens entre ledit dispositif d'interface et ledit premier dispositif serveur. Avantageusement dans ce cas, ladite communication depuis le premier dispositif serveur vers le dispositif d'interface inclut la transmission des données personnelles cryptographiques chiffrées.

Avantageusement, ledit dispositif d'interface choisit un premier entier correspondant à un premier élément d'un groupe prédéfini et ledit premier dispositif serveur choisit un deuxième entier correspondant à un deuxième élément dudit groupe, par exemple de la forme $g^x \bmod p$, puis ledit dispositif d'interface et ledit premier dispositif serveur se transmettent mutuellement lesdits premier et deuxième éléments, ledit dispositif d'interface et ledit premier dispositif serveur produisant chacun ladite au moins une clé de chiffrement par combinaison de l'entier choisi par lui-même et de l'élément reçu par lui-même, ledit premier élément du groupe étant transmis audit premier dispositif serveur sous une forme chiffrée au moyen d'une trace discriminante qui dérive dudit code entré par l'utilisateur dans le dispositif d'interface selon ladite fonction déterministe, ledit premier élément du groupe étant déchiffré par ledit premier dispositif serveur au moyen de ladite donnée personnelle de vérification de code, ledit deuxième élément du groupe étant transmis audit dispositif d'interface sous une forme symétriquement chiffrée au moyen de ladite donnée personnelle de vérification de code, ledit deuxième élément du groupe étant déchiffré par ledit dispositif d'interface au moyen de ladite trace discriminante. Ainsi, un protocole PBKE sur le protocole Diffie-Hellman permet de récupérer les données cryptographiques personnelles chiffrées sur le serveur distant avec authentification par mot de passe et résistance aux attaques par dictionnaire hors ligne.

De préférence, lesdits premier et deuxième éléments du groupe sont chiffrés avec un protocole de chiffrement symétrique qui est choisi de manière qu'une tentative de déchiffrement d'un desdits éléments du groupe selon ledit protocole produise toujours un élément dudit groupe, quelle que soit la clé utilisée dans ladite tentative.

De préférence, lesdits premier et deuxième éléments du groupe sont chiffrés avec un protocole de chiffrement symétrique qui est

choisi de manière que ledit entier ne puisse pas être obtenu à partir de l'élément du groupe correspondant chiffré. Ainsi, les attaques par dictionnaire hors ligne d'un faux serveur ou d'un attaquant interceptant toutes les communications sont rendues essentiellement impossibles.

Selon un mode de réalisation particulier, ledit premier élément du groupe, respectivement ledit deuxième élément du groupe, est chiffré avec un protocole de chiffrement symétrique qui comprend l'étape consistant à composer ledit élément par une loi de composition dudit groupe avec l'image de ladite trace discriminante, respectivement l'image de ladite donnée personnelle de vérification de code, par une fonction à valeurs dans ledit groupe.

De préférence, ladite étape d'utilisation comprend l'étape consistant à authentifier ledit utilisateur auprès dudit au moins un deuxième dispositif serveur au moyen de données d'authentification dudit utilisateur incluses dans lesdites données cryptographiques personnelles. Par exemple, les données d'authentification comportent un certificat numérique de l'utilisateur.

Selon un mode de réalisation particulier de l'invention, ladite étape d'utilisation comprend les étapes consistant à :

recevoir des données de contenu entrées par ledit utilisateur dans ledit dispositif d'interface,

chiffrer lesdites données de contenu au moyen d'au moins une clé de chiffrement incluse dans lesdites données cryptographiques personnelles,

envoyer lesdites données de contenu chiffrées audit au moins un deuxième dispositif serveur pour stocker lesdites données de contenu chiffrées dans ledit deuxième dispositif serveur et/ou les transmettre à un destinataire.

Ce mode de réalisation peut être appliqué à l'accès en écriture à une banque de données personnelles et à l'envoi de courrier électronique chiffré. Par exemple, la clé de chiffrement est une clé cryptographique forte, par exemple supérieure ou égale à 128 bits, pour chiffrer symétriquement lesdites données de contenu.

Selon un autre mode de réalisation particulier de l'invention, ladite étape d'utilisation comprend les étapes consistant à :

envoyer une deuxième requête de lecture désignant des données de contenu depuis ledit dispositif d'interface audit au moins un deuxième

dispositif serveur,
recevoir lesdites données de contenu chiffrées depuis ledit au moins un deuxième dispositif serveur dans ledit dispositif d'interface,
déchiffrer lesdites données de contenu au moyen d'au moins une clé de déchiffrement incluse dans lesdites données personnelles cryptographiques.

Ce mode de réalisation peut être appliqué à la réception de courrier électronique chiffré, à la réception de données de contenu audio et/ou vidéo, et à l'accès en lecture à une banque de données personnelles, lesdites données de contenu étant des données personnelles qui ont été préalablement chiffrées au moyen desdites données personnelles cryptographiques et stockées par ledit utilisateur dans ledit deuxième dispositif serveur. Ce mode de réalisation permet aussi, dans le cas où le deuxième serveur est également un serveur de clés similaire au premier, d'accéder à des clés privées de l'utilisateur stockées sous forme chiffrée sur le deuxième serveur. La connexion au deuxième serveur s'effectue alors à l'aide des données cryptographiques personnelles récupérées sur le premier serveur. Ainsi, la protection des clés privées est accrue en rendant leur récupération dépendante de la réussite d'une série de connexions préalables à plusieurs serveurs de clés successifs.

Selon un autre mode de réalisation, ladite première requête de lecture inclut une trace discriminante dudit code entré et lesdites données personnelles de chaque utilisateur comprennent des données personnelles de vérification de code pour vérifier que ledit code entré correspond audit code authentique de l'utilisateur, lesdites données personnelles cryptographiques chiffrées dudit utilisateur n'étant reçues dans ledit dispositif d'interface que si ledit code entré correspond audit code authentique de l'utilisateur. Une trace discriminante du code est une trace qui permet de différencier deux codes différents. Elle peut être le code lui-même - mais ce mode de réalisation est déconseillé pour des raisons de sécurité - ou une image du code par une fonction cryptographique déterministe et résistante aux collisions, c'est-à-dire une fonction qui présente une propriété d'injectivité au sens calculatoire du terme, dans la mesure où il est techniquement impossible de construire deux antécédents d'une même image.

La trace discriminante sert à prouver que l'utilisateur connaît le code authentique, autant que possible sans divulguer le code authentique.

Ainsi, le code entré par l'utilisateur du dispositif d'interface sert à authentifier celui-ci auprès du premier serveur et les données personnelles cryptographiques ne sont envoyées à l'utilisateur que lorsqu'il a fait la preuve qu'il connaît le code authentique, ce qui empêche un tiers de recevoir les données personnelles cryptographiques chiffrées pour tenter de casser leur chiffrement par des essais systématiques. Par exemple, les données personnelles de vérification de code peuvent comporter un identifiant de l'utilisateur et le mot de passe authentique ou une donnée dérivée de celui-ci.

Avantageusement, le procédé selon l'invention comporte les étapes consistant à :

calculer ladite trace discriminante en tant que transformée non inversible du code entré dans ledit dispositif d'interface,

lesdites données personnelles de vérification de code stockées dans le premier dispositif serveur comprenant une transformée similaire dudit code authentique. Les données personnelles de vérification de code stockées dans le premier dispositif serveur découlent d'une transformation non inversible du code authentique, de sorte que le code authentique de l'utilisateur ne peut être retrouvé à partir des données personnelles de vérification de code stockées dans le premier dispositif serveur. On évite ainsi que même le premier dispositif serveur et ses exploitants ne puissent retrouver facilement le code authentique.

Pour prouver que l'utilisateur connaît le code authentique, on peut aussi envisager d'utiliser un protocole de preuve cryptographique à divulgation nulle, c'est-à-dire un protocole de preuve dont on peut prouver mathématiquement qu'il n'apporte aucune information sur la donnée dont il prouve la connaissance. Cette preuve à divulgation nulle présente cependant deux problèmes : le premier est qu'elle n'évite pas à elle seule les attaques actives où un adversaire intercepte et modifie toutes les communications entre l'utilisateur et le serveur. Le deuxième est qu'elle nécessite deux phases : une première d'authentification, et une seconde d'envoi des clés chiffrées, et donc plusieurs allers-retours réseau.

De préférence, le procédé selon l'invention comporte l'étape consistant à imposer un délai minimum prédéterminé entre le traitement de deux occurrences successives de ladite première requête de lecture au niveau du premier dispositif serveur, sous peine de ne pas tenir compte de l'occurrence la plus tardive. De cette manière, on rend essentiellement impossible une tentative d'obtention des données personnelles par une attaque « par dictionnaire en ligne » consistant à envoyer une multitudes d'occurrences successives de la première requête de lecture en variant systématiquement le code inclus dedans.

En effet, un mot de passe n'a qu'une faible sécurité : il est sensible aux attaques par dictionnaire. Une attaque par dictionnaire consiste à supposer que le mot de passe est issu d'une liste de mots de passe possibles, et à essayer chaque mot de cette liste. Un mot de passe typique (c'est-à-dire un mot de passe qu'un utilisateur pourra mémoriser) sera typiquement trouvable en quelques centaines de milliers d'essais. On distingue deux types d'attaques par dictionnaire :

- les attaques en ligne : chaque essai nécessite une interaction avec une entité connaissant légitimement le mot de passe (par exemple un serveur informatique sur réseau) ;
- les attaques hors ligne : l'attaquant possède toutes les données nécessaires pour "essayer" chaque mot de passe sur ses propres ordinateurs et en vérifier la validité.

Les attaques hors ligne sont fatales, car seule la puissance de l'ordinateur de l'attaquant limite le nombre d'essais qu'il pourra mener à chaque seconde ; un débit réaliste est de l'ordre de 10 000 essais par seconde, ce qui signifie que le mot de passe sera trouvé en quelques minutes. Les attaques en ligne, en revanche, peuvent être contrées facilement : il suffit pour le serveur contacté de limiter le nombre d'essais de l'attaquant, par exemple en imposant un délai à chaque réponse, ou en refusant de répondre après un certain nombre d'essais infructueux.

De préférence, le procédé selon l'invention comporte une étape consistant à surveiller systématiquement les communications impliquant ledit premier dispositif serveur. En effet, les requêtes de lecture reçues par le premier dispositif serveur et les données cryptographiques envoyées en réponse par le premier dispositif serveur

sont peu nombreuses et peu volumineuses, ce qui rend un tel contrôle possible sans coût excessif. Avantageusement, le premier dispositif serveur est exclusivement dédié à stocker les données personnelles des utilisateurs et mettre celles-ci à disposition de leurs propriétaires lorsque ceux-ci le requièrent, au début d'une session, ce qui contribue à limiter le volume desdites communications.

Avantageusement, le procédé selon l'invention comporte l'étape consistant à :

contrôler l'intégrité des données personnelles cryptographiques reçues depuis ledit premier dispositif serveur au moyen de données de contrôle d'intégrité jointes auxdites données personnelles cryptographiques reçues depuis ledit premier dispositif serveur. Ainsi, on peut détecter toute altération des données personnelles cryptographiques au cours de leur transmission depuis le premier dispositif serveur.

De préférence, le procédé selon l'invention comporte l'étape consistant à authentifier ledit premier dispositif serveur auprès dudit dispositif d'interface avant l'envoi de ladite première requête de lecture. De ce fait, on empêche un faux premier dispositif serveur de recevoir la requête, qui peut contenir la trace discriminante du code authentique de l'utilisateur, et donc de pouvoir monter une attaque « par dictionnaire » portant sur le code authentique.

Avantageusement, le procédé selon l'invention comporte l'étape consistant à établir une communication confidentielle avec le premier dispositif serveur avant l'envoi de ladite première requête de lecture depuis le dispositif d'interface. On empêche ainsi tout tiers interceptant les communications entre le premier dispositif serveur et le dispositif d'interface de lire la première requête, qui peut contenir la trace discriminante du code authentique de l'utilisateur, et donc de pouvoir monter une attaque « par dictionnaire » portant sur le code authentique. Par exemple, l'authentification du premier dispositif serveur et/ou l'établissement d'une communication confidentielle sont réalisés en utilisant un certificat numérique du premier dispositif serveur et le protocole SSL.

De préférence, le procédé selon l'invention comporte une étape d'inscription consistant à :

mettre à disposition des données personnelles cryptographiques dans

ledit dispositif d'interface,
recevoir un code authentique entré par ledit utilisateur dans ledit dispositif d'interface,
chiffrer lesdites données personnelles cryptographiques au moyen dudit code authentique,
envoyer lesdites données personnelles cryptographiques chiffrées depuis ledit dispositif d'interface audit premier dispositif serveur pour stocker lesdites données personnelles cryptographiques chiffrées dans ledit premier dispositif serveur,
supprimer lesdites données personnelles cryptographiques et ledit code authentique dudit dispositif d'interface.

Avantageusement, l'étape d'inscription comporte aussi les étapes consistant à :
former des données personnelles de vérification de code à partir dudit code authentique,
envoyer lesdites données personnelles de vérification de code depuis ledit dispositif d'interface audit premier dispositif serveur pour stocker lesdites données personnelles de vérification de code dans ledit premier dispositif serveur.

La mise à disposition des données personnelles cryptographiques peut être effectuée par lecture desdites données sur un support comme une carte à puce ou par génération desdites données dans le dispositif d'interface à partir d'un générateur de nombres aléatoires.

Par exemple, le code authentique est un mot de passe mémorisé par l'utilisateur qui est transformé en une clé cryptographique dans le dispositif d'interface pour chiffrer symétriquement au moins certaines des données cryptographiques personnelles.

De préférence, le procédé selon l'invention comporte une étape consistant à rejeter ledit code authentique entré par l'utilisateur lorsque ledit code remplit des critères d'évidence prédéfinis. Ainsi, on assure dès l'étape d'inscription que le code authentique ne peut pas être un code évident, ce qui renforce la sûreté des données stockées sur le premier dispositif serveur contre les attaques « par dictionnaire » fomentées pour obtenir frauduleusement le code authentique et les données personnelles cryptographiques, y compris par les personnes ayant le contrôle du premier dispositif serveur. Par exemple, les critères

d'évidence prédéfinis peuvent imposer un nombre de caractères minimum, un nombre de caractères non alphanumériques minimum, et exclure des chaînes de caractères courantes, comme les dates, prénoms, etc.

De préférence, le procédé selon l'invention comporte l'étape consistant à authentifier ledit premier dispositif serveur auprès dudit dispositif d'interface avant l'envoi desdites données personnelles cryptographiques chiffrées. Avantageusement, le procédé selon l'invention comporte l'étape consistant à établir une communication confidentielle entre le dispositif d'interface et le premier dispositif serveur avant l'envoi desdites données personnelles cryptographiques chiffrées. De ce fait, on empêche tout tiers se faisant passer pour le premier dispositif serveur ou espionnant les échanges entre le premier dispositif serveur et le dispositif d'interface de recevoir les données personnelles cryptographiques chiffrées, et donc de pouvoir monter une attaque « par dictionnaire » portant sur le code authentique pour déchiffrer lesdites données personnelles cryptographiques.

L'invention fournit également un dispositif d'interface pour échanger de manière protégée des données de contenu en ligne, comportant un moyen pour recevoir un code entré par un utilisateur,
un moyen pour envoyer une première requête de lecture depuis ledit dispositif d'interface à un premier dispositif serveur dans lequel sont stockées des données personnelles cryptographiques respectives d'une pluralité d'utilisateurs, lesdites données personnelles cryptographiques de chaque utilisateur étant chiffrées au moyen d'un code authentique respectif dudit utilisateur,
un moyen pour recevoir les données personnelles cryptographiques chiffrées dudit utilisateur depuis ledit premier dispositif serveur,
un moyen pour déchiffrer lesdites données personnelles cryptographiques au moyen dudit code entré, lorsque ledit code entré correspond audit code authentique de l'utilisateur,
caractérisé par le fait qu'il comporte :
des moyens pour utiliser lesdites données personnelles cryptographiques afin de protéger un échange de données de contenu entre ledit dispositif d'interface et au moins un deuxième dispositif serveur,

un moyen pour supprimer ledit code et lesdites données cryptographiques personnelles dudit dispositif d'interface.

Le dispositif d'interface selon l'invention peut être réalisé en tant qu'appareil dont la conception matérielle est spécifique à cette fin, ou en tant qu'appareil de conception matérielle classique, par exemple un micro-ordinateur générique, programmé au moyen d'un programme d'ordinateur spécifique à cette fin, ou en tant que combinaison des deux. Le dispositif d'interface selon l'invention peut aussi être réalisé en tant que programme d'ordinateur. Au sens de l'invention, un programme d'ordinateur comporte des codes d'instruction aptes à être lus ou stockés sur un support et exécutables par un ordinateur ou un appareil similaire.

Selon un mode de réalisation particulier de l'invention, le dispositif consiste en un programme de gestion de courrier électronique, lesdits moyens d'utilisation des données personnelles cryptographiques comprenant un module cryptographique pour signer, chiffrer et/ou déchiffrer des courriers électroniques à l'aide d'au moins certaines desdites données cryptographiques personnelles.

Selon un autre mode de réalisation particulier de l'invention, le dispositif consiste en un module d'extension adapté à un programme de gestion de courrier électronique comprenant un module cryptographique pour signer, chiffrer et déchiffrer des courriers électroniques, lesdits moyens d'utilisation des données personnelles cryptographiques comprenant un moyen pour fournir audit module cryptographique au moins certaines desdites données cryptographiques personnelles.

De manière séparée du dispositif ci-dessus ou de manière intégrée à celui-ci, l'invention fournit également un dispositif d'interface d'inscription, caractérisé par le fait qu'il comporte :

un moyen pour mettre à disposition des données personnelles cryptographiques dans ledit dispositif d'interface,

un moyen pour recevoir un code authentique entré par ledit utilisateur dans ledit dispositif d'interface,

un moyen pour chiffrer lesdites données personnelles cryptographiques au moyen dudit code authentique,

un moyen pour envoyer lesdites données personnelles cryptographiques

chiffrées depuis ledit dispositif d'interface à un premier dispositif serveur pour stocker lesdites données personnelles cryptographiques chiffrées dans ledit premier dispositif serveur, dans lequel sont stockées des données personnelles cryptographiques respectives d'une pluralité d'utilisateurs, lesdites données personnelles cryptographiques de chaque utilisateur étant chiffrées au moyen d'un code authentique respectif dudit utilisateur,

un moyen pour supprimer lesdites données personnelles cryptographiques et ledit code authentique dudit dispositif d'interface.

L'invention sera mieux comprise, et d'autres buts, détails, caractéristiques et avantages de celle-ci apparaîtront plus clairement au cours de la description suivante de plusieurs modes de réalisation particuliers de l'invention, donnés uniquement à titre illustratif et non limitatif, en référence au dessin annexé. Sur ce dessin :

- la figure 1 est un schéma de principe d'un système pour la mise en œuvre du procédé d'échange de données selon l'invention,
- la figure 2 est un diagramme représentant une étape d'inscription du procédé d'échange de données selon l'invention,
- la figure 3 est un diagramme représentant une session d'utilisation du procédé d'échange de données selon l'invention,
- la figure 4 représente une application du procédé selon l'invention à une banque de données personnelles,
- la figure 5 représente une application du procédé selon l'invention à la gestion de courrier électronique sécurisé,
- la figure 6 représente une application du procédé selon l'invention à la diffusion audiovisuelle,
- la figure 7 représente un autre mode de réalisation de la session d'utilisation.

En référence à la figure 1, un réseau de transport de données 1, par exemple l'Internet, relie entre eux des serveurs de contenu 2a et 2b offrant des services en ligne, un serveur de clés 3 et des dispositifs

d'interface 4a, 4b, 4c pour utiliser les services offerts par les serveurs de contenu 2a et 2b. Les dispositifs d'interface 4a, 4b sont des ordinateurs classiques comportant une mémoire, une unité de traitement des données et des périphériques d'entrée/sortie et de stockage. Ils sont reliés au réseau 1 par des liaisons filaires 5a et 5b. Le dispositif d'interface 4c est un téléphone cellulaire comportant également une mémoire, une unité de traitement des données, un clavier 6 et un écran 7. Il est relié au réseau 1 par l'intermédiaire d'une liaison radio 5c avec une station d'émission/réception 1a intégrée au réseau 1. Bien que seulement deux serveurs de contenu et trois dispositifs d'interface soient représentés, le système peut comporter un très grand nombre des uns et/ou des autres. L'invention n'est pas limitée à cet égard. De plus, un même ordinateur peut constituer simultanément plusieurs serveurs, ceux-ci étant mis en œuvre sous une forme logicielle et ayant chacun une adresse spécifique sur le réseau 1. A ce titre, le serveur de clés 3 peut être mis en oeuvre par le même ordinateur qu'un serveur de contenu.

Les serveurs de contenu 2a et 2b servent à fournir aux utilisateurs des dispositifs d'interface 4a, 4b, 4c des services impliquant des données de contenu. Par exemple, les serveurs de contenu 2a et 2b peuvent comprendre des serveurs de sites sur la Toile, des serveurs de courrier électronique, des serveurs de données audio/vidéo, des serveurs de fax, des serveurs de transfert de fichiers par protocole FTP, des serveurs de liste de diffusion, des serveurs de discussion en temps réel IRC, des serveurs d'information, des serveurs de commerce électronique, etc.

Le serveur de clés 3 est un serveur exclusivement dédié à stocker des données personnelles cryptographiques et des données personnelles de vérification de code d'une pluralité d'utilisateurs enregistrés auprès du serveur de clés 3 ou de son exploitant, et à transmettre à tout dispositif d'interface depuis lequel un utilisateur enregistré en fait la demande les données personnelles cryptographiques de cet utilisateur.

Pour renforcer la sécurité des données personnelles stockées sur le serveur de clés 3, celui-ci est de préférence situé dans un lieu protégé par un blindage et/ou des restrictions d'accès. De plus, le serveur de clés 3 est autant que possible physiquement fermé, notamment par

fermeture des ports de communication non indispensables. Du fait des fonctions restreintes remplies par le serveur de clés 3, le nombre d'accès à celui-ci et le volume des données qu'il échange sont assez limités. Au contraire, les données de contenu sont généralement volumineuses et peuvent faire l'objet d'une multitude d'accès simultanés, de sorte que le volume des échanges entre chaque serveur de contenu 2a ou 2b et le réseau 1 est généralement bien plus grand qu'entre le serveur de clés 3 et le réseau 1, ce qui est symbolisé par l'épaisseur des traits de liaison entre les serveurs respectifs et le réseau 1.

La petitesse des flux de données entrants et sortants du serveur de clés 3 permet qu'un système de surveillance 8, représenté symboliquement sur la figure 1, surveille en temps réel les communications entre le serveur de clés 3 et le réseau 1, par exemple en surveillant le journal de bord du serveur de clés 3.

Pour s'enregistrer auprès du serveur de clés 3, un utilisateur effectue depuis un dispositif d'interface 4a-c une étape d'inscription qui va maintenant être décrite en référence à la figure 2.

A l'étape 10, l'utilisateur lance une application d'inscription sur un dispositif d'interface, par exemple un micro-ordinateur relié au réseau 1.

A l'étape 11, le dispositif d'interface engendre des données cryptographiques personnelles pour l'utilisateur. Pour pouvoir effectuer un chiffrement/déchiffrement symétrique de données de contenu, une clé privée KS est engendrée au moyen d'un générateur pseudo-aléatoire sûr embarqué dans le dispositif d'interface et utilisant une donnée d'initialisation aléatoire provenant d'une mesure physique. Plusieurs méthodes existent pour obtenir une telle donnée d'initialisation, par exemple en demandant à l'utilisateur de frapper au hasard des touches sur un clavier du dispositif d'interface et en chronométrant précisément les intervalles de temps entre deux frappes successives. Pour pouvoir mettre en oeuvre une méthode de chiffrement à clé publique, une paire de clés formée d'une clé publique KB et d'une clé privée correspondante KR est engendrée. Toutes ces clés sont choisies suffisamment longues, par exemple de 128 bits ou plus, pour assurer une haute sécurité cryptographique.

A l'étape 12, l'utilisateur fait certifier sa clé publique KB par une autorité de certification, qui peut être une entité indépendante non représentée ou le serveur de clés 3, selon une technique connue. Une telle certification sert à prouver qu'une clé publique KB appartient à cette personne donnée, qui est seule à posséder la clé privée KR correspondante. L'utilisateur obtient ainsi un certificat numérique A qui contient la clé publique KB et différentes données d'identification de son propriétaire, comme le nom de l'utilisateur, son adresse, son âge, etc. Par exemple, le certificat numérique A est au format standardisé X.509 utilisable dans un protocole de chiffrement SSL. La clé privée KR, le certificat numérique A et la clé symétrique KS constituent les données cryptographiques personnelles de l'utilisateur.

Les étapes 11 et 12 ne sont qu'un exemple de mise à disposition des données cryptographiques personnelles de l'utilisateur dans la mémoire du dispositif d'interface. En variante, l'utilisateur pourrait avoir obtenu de telles clés préalablement, par exemple sur un support tel qu'une carte à puce, et charger ces données dans la mémoire du dispositif d'interface à l'aide d'un lecteur approprié. Cette étape de mise à disposition ne devant être effectuée qu'une seule fois, la carte à puce pourrait ensuite être mise en sécurité dans un coffre-fort pour servir de copie de sauvegarde.

Les données cryptographiques personnelles au sens de l'invention ne sont pas limitées à la combinaison de clés précitée. Ces données pourraient aussi se limiter à une unique clé privée ou, au contraire, être plus nombreuses. Toutefois, il est préférable de prévoir des clés distinctes pour chaque fonction. Dans le cas présent, le couple formé du certificat A et de la clé privée KR sert à la fonction d'authentification de l'utilisateur et la clé privée KS à la fonction de chiffrement/déchiffrement des données de contenu.

A l'étape 14, l'utilisateur est invité à entrer un identifiant personnel N_i tel que son nom ou un pseudonyme, et un mot de passe personnel dans le dispositif d'interface. Ce mot de passe est choisi par l'utilisateur. Si le mot de passe saisi comporte moins de huit caractères ou moins de deux caractères non alphanumériques, il est rejeté automatiquement et l'invitation est réitérée. Lorsqu'un mot de passe acceptable est entré, l'utilisateur est invité à le confirmer en le saisissant

une deuxième fois, ceci afin d'assurer que l'utilisateur n'a pas commis d'erreur dans son choix et connaît son mot de passe de manière certaine. Le mot de passe, une fois confirmé, est mémorisé comme mot de passe authentique P de l'utilisateur.

A l'étape 16, le mot de passe authentique P est transformé de manière non inversible en une clé de chiffrement symétrique KP par application d'une fonction de hachage à la concaténation de l'identifiant N et du mot de passe authentique P de l'utilisateur. Par exemple, la fonction de hachage utilisée est la fonction SHA définie par le standard FIPS 180.

A l'étape 18, une clé personnelle de vérification de mot de passe VP est calculée par une transformation injective non inversible du mot de passe authentique P. Par exemple, VP résulte de l'application d'une fonction de hachage à la clé de chiffrement symétrique KP.

A l'étape 20, la clé privée KR et le certificat numérique A sont chiffrés symétriquement au moyen de la clé symétrique KS. La clé symétrique KS est chiffrée symétriquement au moyen de la clé de chiffrement KP résultant du mot de passe authentique P. En variante, on pourrait chiffrer toutes les données personnelles cryptographiques au moyen de la clé de chiffrement KP. Dans tous les cas, les données personnelles cryptographiques de l'utilisateur sont considérées chiffrées par le mot de passe authentique P, c'est-à-dire qu'elles sont chiffrées d'une manière telle que le mot de passe authentique P est nécessaire pour les déchiffrer.

A l'étape 22, le dispositif d'interface établit une communication sécurisée avec le serveur de clés 3 via le réseau 1. Pour cela, on peut utiliser le protocole standard SSL qui assure la confidentialité et l'intégrité des données échangées entre le dispositif d'interface et le serveur de clés 3, ainsi que l'authentification du serveur de clés 3 auprès du dispositif d'interface. Le protocole SSL comporte plusieurs variantes, dont l'une est décrite ci-dessous.

Le dispositif d'interface contacte le serveur de clés 3 et lui signifie son intention de communiquer avec lui. Le serveur de clés 3 choisit aléatoirement une paire de clés formée d'une clé publique PA et d'une clé privée KV, correspondant à l'algorithme standard Diffie-Hellman. Le serveur de clés 3 possède un certificat public CA qui

contient une autre clé publique SP du serveur de clés 3, à laquelle correspond une clé privé respective SR du serveur de clés 3. Le serveur de clés 3 transmet au dispositif d'interface le certificat public CA, la clé publique PA et une signature électronique de la clé publique PA par la clé privée SR. Le dispositif d'interface vérifie la signature du certificat CA à l'aide de la clé publique de l'autorité de certification qui l'a signé, et vérifie la signature de la clé publique PA à l'aide de la clé publique SP. Le dispositif d'interface choisit aléatoirement une paire de clés formée d'une clé publique PB et d'une clé privée KW, selon l'algorithme Diffie-Hellman, et transmet la clé publique PB au serveur de clés 3. Le serveur de clés 3 calcule une clé de session KT en fonction de la clé publique PB et de sa clé privée KV. Le dispositif d'interface calcule une clé de session KT en fonction de la clé publique PA et de sa clé privée KW. L'algorithme Diffie-Hellman assure que le dispositif d'interface et le serveur de clés 3 calculent la même clé de session KT, c'est-à-dire qu'ils obtiennent de manière différente le même résultat de calcul. Ce résultat n'est pas calculable sans la connaissance d'au moins une des clés privées KV et KW.

Plus précisément, selon le protocole Diffie-Hellman, deux parties, notées A et B, veulent établir une clé de session commune entre elles. Certains paramètres sont connus publiquement et ne sont pas spécifiques à A ni à B :

- p, un nombre premier de grande taille (par exemple 1024 bits) ;
- q, un nombre entier divisant p - 1, et de taille moyenne (par exemple 160 bits) ;
- g, un entier modulo p générant un sous-groupe d'ordre q de Z^*_p.

On travaille ici modulo l'entier p, sur le groupe Z^*_p des nombres inversibles modulo p. Le sous-groupe engendré par g est constitué de toutes les puissances de g modulo p ; ce sous-groupe comporte q valeurs différentes.

Le protocole Diffie-Hellman est le suivant :

- A choisit aléatoirement un entier a modulo q ; ce choix est réalisé uniformément entre 0 et q - 1 (inclus).
- A calcule g^a mod p et envoie le résultat à B.
- B choisit aléatoirement un entier b modulo q ; ce choix est réalisé uniformément entre 0 et q - 1 (inclus).

- B calcule g^b mod p et envoie le résultat à A.
- A utilise a et g^b mod p pour calculer la valeur $K_A = (g^b)^a \text{mod } p$.
- B utilise b et g^a mod p pour calculer la valeur $K_B = (g^a)^b \text{mod } p$.

Il s'avère, par commutativité de la multiplication modulo p, que $K_A = K_B = g^{ab}$ mod p. Cette valeur commune est la clé de session.

La sécurité du protocole Diffie-Hellman repose sur la difficulté de retrouver l'entier a, car a est choisi aléatoirement, à partir de g^a mod p. Ce problème est connu sous le nom de logarithme discret. Si p est de taille suffisante (par exemple 1024 bits) et que a est choisi dans un ensemble suffisamment vaste (c'est-à-dire que q est assez grand - au moins 160 bits), alors le logarithme discret est au-delà de la technologie existante.

La description originale du protocole Diffie-Hellman utilise les entiers modulo p, mais peut être étendue à n'importe quel groupe sur lequel l'équivalent du logarithme discret est un problème "difficile", c'est-à-dire non résoluble par les moyens informatiques actuels. Un exemple de tel groupe est une courbe elliptique : une courbe elliptique est un ensemble de points, chaque point ayant deux coordonnées dans un corps fini. On peut définir sur cette courbe une règle d'addition de deux points, qui fournit un troisième point de la courbe et qui respecte les conditions nécessaires pour être une loi de groupe.

Le protocole Diffie-Hellman suppose que les échanges sont intègres, c'est-à-dire que les données envoyées par A et par B ne sont pas modifiées sur le chemin par un attaquant. Le protocole Diffie-Hellman ne réalise pas d'authentification des deux parties. C'est pourquoi il est nécessaire de disposer du certificat public CA du serveur de clés dans le protocole SSL susmentionné.

A ce stade, les deux interlocuteurs ont mis en commun une clé temporaire KT qu'ils sont seuls à connaître. Par ailleurs, le serveur de clés 3 s'est authentifié auprès du dispositif d'interface grâce à la preuve d'identité que constitue le certificat CA. Tous leurs échanges ultérieurs sont effectués, au niveau de l'émetteur, en chiffrant symétriquement avec la clé de session KT les données à envoyer et, au niveau du récepteur, en déchiffrant avec la clé de session KT les données reçues. Le contenu des données ainsi échangées est parfaitement secret vis-à-vis de tout dispositif intermédiaire de transport.

Dans le protocole décrit ci-dessus, le client, c'est-à-dire le dispositif d'interface ou son utilisateur, n'est pas encore authentifié auprès du serveur de clés 3. On peut souhaiter authentifier le client auprès du serveur de clés 3 lors de la procédure d'inscription, notamment pour éviter qu'un tiers puisse écraser ou modifier le compte d'un utilisateur préalablement inscrit. Cette authentification peut être effectuée par toute méthode connue permettant d'identifier le client auprès de l'autorité d'enregistrement ayant le contrôle du serveur de clés 3.

Par exemple, l'autorité d'enregistrement peut exiger une rencontre physique avec un futur utilisateur avant son inscription pour prendre connaissance de son identité par présentation de documents officiels à un guichet d'inscription. A cette occasion, l'autorité d'enregistrement peut attribuer et communiquer confidentiellement au futur utilisateur un mot de passe, qui devra être entré par l'utilisateur sur le dispositif d'interface pour établir la connexion SSL précitée.

En variante ou en combinaison avec l'utilisation d'un mot de passe attribué par l'autorité d'enregistrement, on peut également utiliser le protocole SSL de manière bi-authentifiée : pour cela, le dispositif d'interface fait usage de son certificat numérique A contenant la clé publique KB. Le dispositif d'interface signe la clé publique PB à l'aide de la clé privée KR et envoie au serveur de clés 3 la clé publique PB signée et le certificat A. Le serveur de clés 3 vérifie la signature du certificat A à l'aide de la clé publique de l'autorité de certification qui l'a signé, et vérifie la signature de la clé publique PB à l'aide de la clé publique KB. Ainsi, l'utilisateur du dispositif d'interface est authentifié auprès du serveur de clés 3 grâce à la preuve d'identité que constitue le certificat A.

De préférence, tous les paquets de données M échangés entre le dispositif d'interface et le serveur de clés 3 sont munis de moyens de contrôle d'intégrité permettant au destinataire de vérifier que les données n'ont pas été altérées entre leur émission et leur réception. Un exemple de tels moyens de contrôle, qui s'applique notamment lorsque le chiffrement des données échangées est réalisé à l'aide d'une fonction de chiffrement symétrique par bloc, consiste à concaténer avec le paquet de données M proprement dit, avant son chiffrement avec la clé de session

KT, le résultat de l'application d'une fonction de hachage au paquet de données, soit par exemple SHA(M). Après déchiffrement, le destinataire du paquet de données peut ainsi vérifier que les données qu'il a reçues présentent bien une structure de type M//SHA(M), ce qui permet au destinataire de détecter une éventuelle altération des données au cours de la communication et de la signaler à l'expéditeur, pour qu'il répète l'envoi ou qu'il prenne une autre mesure de sécurité.

Dans ces conditions, à l'étape 24, le dispositif d'interface envoie de manière sécurisée au serveur de clés 3 une requête de création de compte personnel d'utilisateur contenant : l'identifiant N, les données personnelles cryptographiques A, KR, KS chiffrées par le mot de passe authentique P et la clé de vérification de mot de passe VP. Le serveur de clés 3 stocke ces données dans un compte, c'est-à-dire un espace de stockage, réservé à l'utilisateur, par exemple sur un disque dur.

A l'étape 26, le serveur de clés 3 envoie un message de confirmation de la création du compte. Les échanges entre le dispositif d'interface et le serveur de clés 3 sont maintenant terminés pour ce qui concerne l'inscription et la clé de session temporaire KT peut être effacée par les deux interlocuteurs.

A l'étape 28, l'utilisateur ferme l'application d'inscription, ce qui entraîne l'effacement du mot de passe authentique P et de toutes les données personnelles cryptographiques A, KB, KR, KS chiffrées ou non de la mémoire du dispositif d'interface. Aucune donnée confidentielle de l'utilisateur ne reste dans la mémoire du dispositif d'interface, de sorte que l'utilisateur n'est pas lié à ce dispositif particulier et qu'aucun contrôle des accès à ce dernier n'est nécessaire par la suite. Le dispositif d'interface peut être d'accès public, par exemple dans un cybercafé.

L'étape d'inscription permet ainsi à l'utilisateur de stocker sur le serveur de clés 3, qui est accessible depuis tout dispositif d'interface relié au réseau 1, des données personnelles cryptographiques sous une forme chiffrée qu'il est le seul à pouvoir déchiffrer. Le chiffrement obtenu à l'aide de la clé KS est un chiffrement fort qui est réputé inviolable, en raison de la longueur de cette clé. Le chiffrement obtenu à l'aide de la clé KP est généralement moins fort car il dérive directement du mot de passe P qui doit avoir une longueur raisonnable pour être mémorisé par l'utilisateur. Cependant, le mot de passe P n'est stocké sur

aucun support. Il ne peut pas être retrouvé directement à partir de la clé de vérification VP, sauf par une recherche systématique. En outre, une telle recherche systématique ne serait réalisable que par le serveur de clés 3 qui est le seul à stocker la clé de vérification VP. Celle-ci ne transite jamais en clair sur le réseau 1.

Depuis l'étape 10 ci-dessus, on a décrit une procédure d'inscription en ligne assurant l'authentification du serveur de clés 3 et éventuellement l'authentification de l'utilisateur, ainsi que la confidentialité des échanges entre l'utilisateur et le serveur de clés 3. D'autres procédures d'inscription assurant les mêmes garanties sont néanmoins possibles. Par exemple, l'utilisateur peut être conduit par l'autorité d'enregistrement dans une pièce blindée contenant le serveur de clés 3, auquel cas l'authentification du serveur et la confidentialité des communications sont assurées par des moyens non cryptographiques, du seul fait de l'absence de dispositif intermédiaire de communication et de l'isolation physique des interlocuteurs par rapport à l'extérieur.

Par la suite, l'utilisateur peut utiliser ses données personnelles cryptographiques depuis n'importe quel dispositif d'interface relié au réseau 1 et muni d'une application de session adaptée. En référence à la figure 3, on décrit maintenant une session d'utilisation depuis un dispositif d'interface.

A l'étape 30, l'utilisateur lance l'application de session.

A l'étape 32, l'utilisateur est invité à entrer son identifiant N et son mot de passe authentique P. L'utilisateur saisit au clavier un identifiant N' et un mot de passe P'.

A l'étape 34, une clé de chiffrement symétrique KP' est calculée à partir du mot de passe P' et de l'identifiant N' de la même manière que la clé de chiffrement symétrique KP à l'étape 16. Puis une clé VP' est calculée à partir de la clé de chiffrement symétrique KP' de la même manière que la clé de vérification VP à l'étape 18.

A l'étape 36, le dispositif d'interface établit une communication sécurisée avec le serveur de clés 3 via le réseau 1, par exemple en utilisant le protocole standard SSL de manière similaire à l'étape 22. Toutefois, le dispositif d'interface ne dispose pas du certificat A de l'utilisateur à ce stade. Il engendre une paire de clés publique/privée spécialement pour établir cette communication, ce qui

implique que le serveur de clés 3 ne peut pas authentifier l'utilisateur à ce stade. Par cette communication sécurisée, le dispositif d'interface envoie au serveur de clés 3 un requête de lecture contenant l'identifiant N' et la clé VP'.

A l'étape 38, le serveur de clés 3 traite cette requête en identifiant le compte correspondant à l'identifiant N', s'il en existe effectivement un, et en comparant la clé de vérification VP stockée dans ce compte avec le clé VP' reçue dans la requête.

Si le compte n'existe pas, ou si la comparaison est négative, cela indique que l'utilisateur n'a pas entré le couple identifiant/mot de passe authentique d'un utilisateur enregistré. En effet, du fait de la résistance aux collisions de la fonction de hachage, tant que P' diffère de P, VP' diffère de VP. Le serveur de clés 3 envoie alors en réponse un message de refus d'accès, comme indiqué par la flèche 40. On assure ainsi que les données personnelles cryptographiques chiffrées ne seront envoyées qu'à un utilisateur ayant fait la preuve qu'il connaissait le couple identifiant/mot de passe authentique.

Les étapes 32 à 38 sont alors répétées, jusqu'à ce que le serveur de clés 3 reçoive une deuxième occurrence de la requête de lecture. Cependant, pour un même identifiant N', le serveur de clés 3 n'effectue la comparaison prévue à l'étape 38 qu'après un délai supérieur à dix secondes depuis la réception de la première occurrence de la requête de lecture. De ce fait, pour un mot de passe à 8 caractères, essayer automatiquement tous les mots de passe possibles par un envoi automatisé de requêtes successives prendrait un temps déraisonnable, de l'ordre du million d'années.

Lorsque l'étape 38 a permis de reconnaître dans le couple N'/VP' le code authentique N/VP d'un utilisateur enregistré, à l'étape 42, le serveur de clés 3 envoie au dispositif d'interface les données personnelles cryptographiques A, KR, KS chiffrées stockées dans le compte correspondant. Le dispositif d'interface envoie au serveur de clés 3 un accusé de réception, puis la communication entre eux est terminée.

A l'étape 44, le dispositif d'interface déchiffre la clé KS à l'aide de la clé KP' calculée à l'étape 34, puis déchiffre le certificat A et la clé privée correspondante KR à l'aide de la clé KS ainsi obtenue.

A l'étape 46, l'utilisateur accède à des services offerts par un ou plusieurs des serveurs de contenu 2a, 2b depuis le dispositif d'interface. Dans cette étape, les communications entre le ou les serveurs de contenu 2a, 2b et le dispositif d'interface sont protégées par des procédés de chiffrement, de signature électronique et/ou d'authentification en utilisant les données personnelles cryptographiques A, KR, KS. Plusieurs exemples détaillés de cette étape sont décrits ci-dessous.

A l'étape 48, l'utilisation des services étant terminée, l'utilisateur ferme l'application de session, ce qui entraîne l'effacement du mot de passe P', des clés KP' et VP' et de toutes les données personnelles cryptographiques A, KR, KS, chiffrées ou non de la mémoire du dispositif d'interface. Aucune donnée confidentielle de l'utilisateur ne reste dans la mémoire du dispositif d'interface, de sorte que l'utilisateur n'est pas lié à ce dispositif particulier et qu'aucun contrôle des accès à ce dernier n'est nécessaire par la suite. Le dispositif d'interface pour l'étape de session peut aussi être d'accès public, par exemple dans un cybercafé.

Le stockage des données personnelles cryptographiques sur le serveur de clés 3 est plus sûr, du point de vue de la confidentialité et de la durabilité, qu'un stockage local sur le dispositif d'interface ou un stockage sur carte à puce, car le serveur de clés 3 est mieux protégé physiquement et peut être attentivement surveillé.

On décrit maintenant un autre mode de réalisation de l'application de session, en référence à la figure 7. Par convention, le dispositif d'interface est désigné par A et le serveur de clés 3 par B. A et B partagent une infrastructure de données publiques I comprenant des nombres p, q et g convenant pour le protocole de Diffie-Hellman, au moins une fonction de hachage h, par exemple SHA-1, et des protocoles de chiffrement E et F.

Dans A, l'utilisateur (supposé authentique dans l'exemple représenté) entre initialement uniquement son identité N et un mot de passe P. B possède sur son système de stockage interne les données cryptographiques personnelles de l'utilisateur D_A chiffrées symétriquement avec la clé KP déduite du mot de passe P ; on note F la fonction de chiffrement utilisée, c'est-à-dire que B stocke $F_{KP}(D_A)$. A va

récupérer cette donnée D_A. On suppose que B stocke VP = h(N||KP) (mais pas KP) : il s'agit du hachage de la concaténation du nom N et de la clé KP dérivée du mot de passe P.

Le protocole est le suivant :

- A calcule KP et VP à l'aide des donnée N et P entrées par l'utilisateur.
- A choisit un entier a entre 0 et q - 1.
- A calcule $V_A = g^a \bmod p$.
- A envoie à B son nom (N) et $E_{h(N||KP)}(V_A)$.
- B choisit un entier b entre 0 et q - 1.
- B calcule $V_B = g^b \bmod p$.
- B déchiffre $E_{h(N||KP)}(V_A)$ et obtient V_A.
- B calcule $K_s = V_A{}^b \bmod p$.
- B envoie à A les deux messages suivants :
  - $E_{h(N||KP)}(V_B)$
  - $F_{Ks}(F_{KP}(D_A))$
- A déchiffre $E_{h(N||KP)}(V_B)$ et obtient V_B.
- A calcule $K_s = V_B{}^a \bmod p$.
- A déchiffre $F_{Ks}(F_{KP}(D_A))$ et obtient $F_{KP}(D_A)$.
- A déchiffre $F_{KP}(D_A)$ et obtient D_A.

Le système de chiffrement F est un simple système de chiffrement symétrique, utilisant par exemple l'algorithme standard AES. Il peut aussi disposer un système de contrôle d'intégrité (MAC) qui permet de vérifier que le déchiffrement est correct et que les données n'ont pas été altérées.

Le système de chiffrement symétrique E utilisé doit être tel que :

1. Si VP' est différent de VP, le déchiffrement par VP' de $E_{VP}(V_A)$ doit donner un autre élément valide du groupe engendré par g ; autrement dit, l'utilisation d'un autre mot de passe que le bon doit donner une instance valide du problème (mais bien sûr cela ne débouche pas sur la bonne clé de session).

Supposons que A est honnête mais est amené à négocier avec un attaquant C ayant pris la place de B. La première condition sur E protège A. En effet, quand C reçoit $F_{VP}(V_A)$, il peut "essayer" différents mots de passe P' et voir lesquels donnent des déchiffrements "valides",

c'est-à-dire des éléments du groupe engendré par g. Si la condition 1 n'est pas respectée par E, alors cela donne un moyen à C de "tester" hors ligne les mots de passe de son dictionnaire. Après quelques échanges de ce type, C obtiendrait suffisamment de critères de tests pour trouver le mot de passe P dans son dictionnaire.

2. Etant donné $E_{VP}(g^a \bmod p)$, le seul moyen de connaître l'entier a doit être de l'avoir choisi préalablement.

La deuxième condition empêche un attaquant d'utiliser après-coup une session ratée comme test pour une attaque par dictionnaire. Une possibilité pour l'attaquant C (se faisant passer pour B) est de choisir arbitrairement lors de la négociation de clé un mot de passe P" et d'envoyer $E_{VP"}(g^b \bmod p)$. Ensuite, A utilise la clé de session K_s (que C ne connaît pas, sauf s'il a par hasard choisi le bon mot de passe) pour chiffrer un message à destination de C. Le but de C est d'utiliser ce message pour essayer des mots de passe ; pour chacun, noté P', C veut reconstituer le b' tel que $E_{VP'}(g^{b'} \bmod p)$ soit égal à la valeur qu'il a envoyée effectivement à A. Si C peut faire cela, alors C peut, pour chaque mot de passe P', calculer la clé de session K' correspondante, et vérifier si elle déchiffre correctement le message envoyé ensuite par A. Si c'est le cas, alors C a, a posteriori, retrouvé le mot de passe P utilisé par A lors de l'exécution du protocole. Ceci constitue une attaque par dictionnaire hors ligne. La condition 2 sur le chiffrement E empêche justement que cette attaque soit possible.

Un exemple de chiffrement E qui respecte ces conditions est le suivant : on possède une fonction de hachage H dont la sortie est un élément du groupe engendré par g, et on définit $E_\pi(V_A)$ comme la multiplication modulo p de V_A par $H(\pi)$.

Ce mode de réalisation est fondé sur une technique générale appelée échange de clés chiffré ou encrypted key exchange (EKE) qui a été décrite pour la première fois dans un article intitulé "Encrypted Key Exchange : Password-Based Protocols Secure Against Dictionary Attacks", Steven M. Bellovin et Michael Merritt, in Proceedings of the IEEE Symposium on Security and Privacy, Oakland, California, May, 1992, pp. 72-84.

Elle évite toute attaque par dictionnaire hors-ligne, même dans le cas d'un adversaire pouvant intercepter et modifier les

communications, et elle ne nécessite par ailleurs qu'un seul aller-retour réseau.

Le client et le serveur utilisent VP = h(N||KP) comme unique donnée certaine prédéfinie connue du client et du serveur. La clé de session K négociée est utilisée ensuite pour transmettre confidentiellement le paquet de données contenant D_A du serveur vers le client.

Ce protocole a les caractéristiques suivantes :

- Il n'y a qu'une seule passe : une requête du client, une réponse du serveur, et la connexion s'arrête.
- Ni un faux client A parlant à un serveur B légitime, ni un faux serveur B négociant avec un client A légitime, ni un attaquant espionnant ou tentant de modifier une conversation entre un client A légitime et un serveur B légitime, n'apprennent quoi que ce soit permettant de monter une attaque par dictionnaire hors ligne, même partielle, sur le mot de passe P.
- Le serveur B ne connaît pas le mot de passe P (mais il connaît de quoi faire une attaque par dictionnaire hors ligne : h(N||KP) et $F_{KP}(D_A)$).
- A la fin du protocole, si tous les déchiffrements se sont bien déroulés, A a authentifié B, c'est-à-dire qu'il a l'assurance d'avoir parlé à un serveur connaissant h(N||KP).
- A la fin du protocole, B n'a aucune garantie explicite d'avoir parlé avec le vrai client A ; en revanche, B sait que seul le vrai client A pourra tirer quoi que ce soit des données qu'il a envoyées, ce qui constitue une authentification implicite de A. Ainsi, le protocole offre une garantie d'anonymat au client et donc une protection désirable lorsque les connexions de l'utilisateur au serveur de clé 3 relèvent de sa vie privée.

Le fait d'utiliser h(N||KP) au lieu de h(KP) est destiné à empêcher B (au cas où son système de stockage serait compromis par un attaquant) de mener une attaque par dictionnaire hors-ligne parallèlement sur plusieurs mots de passes appartenant à des utilisateurs distincts.

L'application d'inscription et l'application de session peuvent être réalisées sous forme de logiciels indépendants ou sous forme de fonctionnalités distinctes d'un unique logiciel. Il est particulièrement

avantageux de programmer l'application de session et l'application d'inscription à l'aide du système de programmation Java® de Sun Microsystems® car il permet d'obtenir un logiciel, sous une forme binaire et compilée, qui peut fonctionner quelle que soit l'architecture du dispositif d'interface qui l'exécute. On obtient donc des applications de session et d'inscription portables, particulièrement adaptées à une diffusion par téléchargement. De plus, ce système de programmation est disponible pour toutes les architectures majeures et très souvent déjà installé dans les programmes de butinage. Il contient les vérificateurs sémantiques nécessaires qui permettent au dispositif d'interface qui l'exécute de s'assurer qu'aucune opération interdite n'est effectuée, de sorte que l'exécution des applications ainsi obtenues est sûre.

Selon ce mode de réalisation, l'application de session et l'application d'inscription sont exécutables par tout dispositif d'interface ayant un accès générique et standard au réseau 1, sans nécessiter d'accès particulier aux ressources du dispositif d'interface, à part ce que le système de programmation Java® fournit, comme l'interface graphique et l'accès au réseau 1.

De manière alternative, l'application de session peut aussi être implantée sous une forme matérielle et/ou logicielle spécifique dans un type particulier de dispositif d'interface, par exemple dans un modèle de téléphone cellulaire qui sort d'usine avec l'application de session pré-installée.

On décrit maintenant plusieurs exemples de l'étape 46 en référence aux figures 4 à 6. Sur ces figures, la liaison 54 représente à la fois la connexion du dispositif d'interface 50 au réseau 1 et le réseau 1 lui-même ou une partie du réseau 1. Seul un serveur de contenu 2a, 2b ou 2c est représenté à chaque fois car le serveur de clés 3 n'intervient plus. Cependant, on suppose toujours qu'il peut y avoir plusieurs serveurs de contenu et que le dispositif d'interface 50 est apte à communiquer avec le serveur de clés 3, pour pouvoir effectuer les étapes 30 à 44, qui ne seront pas décrites à nouveau.

En référence à la figure 4, le serveur de contenu 2a offre un service de banque de données personnelles à l'utilisateur. Par exemple, une telle banque de données peut être créée avec des logiciels connus sous les noms commerciaux Apache® ou Tomcat®.

Un compte d'utilisateur 52 est réservé dans les moyens de stockage du serveur de contenu 2a, par exemple sur un disque dur ou un disque optique. Ce compte contient des fichiers personnels de l'utilisateur 56, qui sont organisés en une structure hiérarchique. Chaque fichier a été déposé par l'utilisateur sous une forme chiffrée au moyen de la clé symétrique KS, et ce chiffrement comprend un moyen de contrôle d'intégrité des fichiers dérivé de cette même clé. Le serveur de contenu 2a traite ces fichiers comme des suites d'octets sans signification, hormis pour ce qui concerne les méta-données associées (noms et organisation des fichiers). Le serveur de contenu 2a fournit une interface d'accès sous la forme d'un site sur la Toile exécutable depuis le dispositif d'interface 50, qui prend ici la forme d'un micro-ordinateur générique muni d'un programme de butinage ou de navigation classique, comme ceux proposés par les sociétés Netscape® ou Microsoft®.

A l'étape 46, dans cet exemple, l'application de session met les données personnelles cryptographiques A, KR, KS dans un format et à un emplacement mémoire adapté pour que le programme de butinage puisse les lire et les utiliser. A l'aide du programme de navigation, l'utilisateur affiche à l'écran l'interface d'accès au serveur de contenu 2a. Une communication au format standard HTTP est alors établie entre le dispositif d'interface 50 et le serveur de contenu 2a, en utilisant le certificat A et la clé privée correspondante KR de l'utilisateur pour sécuriser cette communication par un protocole SSL, tel qu'il a été décrit à l'étape 22. De préférence, le protocole SSL est utilisée de manière bi-authentifiée, comme décrit à l'étape 22. Ainsi, le dispositif d'interface 50 et le serveur de contenu 2a se sont mutuellement authentifiés, leurs échanges ultérieurs sont confidentiels, et l'intégrité des données transférées peut être contrôlée.

L'interface d'accès au serveur de contenu 2a permet à l'utilisateur de connaître le contenu et la structure de son compte 52, de lire un fichier du compte 52, d'écrire un fichier dans le compte 52, et de déplacer ou effacer un fichier. Pour cela, le dispositif d'interface 50 envoie des requêtes correspondantes 58, selon la technique connue. Ces requêtes ne sont traitées par le serveur de contenu 2a qu'après l'authentification de l'utilisateur au moyen du certificat A, de sorte que les fichiers 56 ne peuvent être lus ou altérés par un tiers. Un tiers ne peut

même pas connaître l'existence de ces fichiers ou les méta-données associées, telles que les noms des fichiers.

Pour stocker un fichier dans le compte 52, l'utilisateur entre ce fichier dans le dispositif d'interface 50, par exemple en créant le fichier depuis un logiciel de traitement de texte, ou en lisant le fichier depuis un support magnétique optique ou autre. Le programme de butinage effectue ensuite un chiffrement symétrique du fichier à l'aide de la clé KS, et envoie le fichier ainsi chiffré dans la requête 58 d'écriture. Le fichier est stocké à l'emplacement désiré par le serveur de contenu 2a. Le serveur de contenu 2a ne possédant pas la clé KS, le contenu des fichiers 56 ainsi stockés est parfaitement secret vis-à-vis du serveur de contenu 2a.

Pour lire un fichier dans le compte 52, l'utilisateur désigne ce fichier par son nom. Le programme de butinage envoie une requête 58 de lecture comprenant ce nom au serveur de contenu 2a. Le serveur de contenu 2a envoie au dispositif d'interface 50 une réponse 60 contenant le fichier correspondant chiffré par la clé KS. Le programme de butinage effectue ensuite un déchiffrement symétrique du fichier à l'aide de la clé KS. Du fait du chiffrement par la clé KS, le sur-chiffrement assuré par le protocole SSL au moyen d'une clé temporaire KT n'est pas indispensable pour garantir la confidentialité des fichiers 56. Cependant, ce sur-chiffrement garantie l'authenticité du serveur et de l'utilisateur tout au long des échanges, ce qui empêche qu'un faux serveur trompe l'utilisateur quant au contenu de son compte ou qu'un faux utilisateur n'altère le contenu du compte 52.

L'utilisateur peut stocker sur le compte 52 toutes sortes de données personnelles, dans des format graphiques, audio, vidéo, texte, etc. Par exemple, le compte 52 contient le carnet d'adresses électroniques de l'utilisateur et ses dossiers de courriers électroniques archivés. Le compte 52 peut aussi contenir d'autres clés cryptographiques de l'utilisateur. Toutes ces données sont conservées de manière confidentielles à cause de leur chiffrement et restent accessibles depuis tout dispositif d'interface muni de l'application de session et d'une application d'accès adaptée, c'est-à-dire par exemple d'un programme de butinage. De plus, le serveur 2a peut assurer de manière très sûre la durabilité des fichiers 56, en effectuant des copies de

sauvegarde qui, du fait du chiffrement fort des fichiers 56, n'entraînent aucun risque intrinsèque.

L'application de session et l'application d'inscription peuvent être réalisées sous la forme d'un ou plusieurs modules logiciels d'extension, encore appelés Plug-in, pour un programme de butinage, par exemple pour le logiciel Netscape Communicator®. Dans ce cas, l'application de session ou l'application d'inscription pourra être lancée par une instruction depuis l'interface du programme de butinage et sera automatiquement fermée lorsque le programme de butinage sera fermé.

De manière alternative, l'application de session et l'application d'inscription peuvent être intégrées à un programme spécifique assurant les fonctions d'accès au serveur 2a.

En référence à la figure 5, on décrit un autre exemple de l'étape 46, dans lequel le service offert est un service de courrier électronique sécurisé. Le serveur 2b est un serveur de courrier électronique pouvant communiquer avec le dispositif d'interface 50 de manière connue en soi, par exemple selon les protocoles SMTP (acronyme pour l'anglais : Simple Mail Transfer Protocol) IMAP (acronyme pour l'anglais : Internet Message Access Protocol) ou POP (acronyme pour l'anglais : Post Office Protocol). A l'étape 46, dans cet exemple, l'application de session met les données personnelles cryptographiques A, KR, KS dans un format et à un emplacement mémoire adapté pour qu'un programme client de gestion de courrier électronique sécurisé puisse les lire et les utiliser.

Il existe des programmes clients de gestion de courrier électronique qui sont sécurisés, c'est-à-dire qu'ils comportent un module cryptographique pour remplir des fonctions de protection, et pour lesquels le stockage des éléments cryptographiques est paramétrable au moyen de modules logiciels d'extension. Des exemples connus sont Outlook Express® de Microsoft® et Netscape Communicator® de Netscape®, dans lequel les opérations de chiffrement et de signature électronique sont effectuées selon le format S/MIME.

L'application de session et/ou l'application d'inscription peut prendre la forme d'un module d'extension pour un tel programme. L'application de session permet ainsi de reconfigurer rapidement le module cryptographique du programme client avec les données

cryptographiques personnelles de l'utilisateur. L'intérêt des modules logiciels d'extension pour ces programmes largement diffusés est de leur ajouter les caractéristiques de l'application d'inscription et/ou de l'application de session sans obliger les utilisateurs à apprendre le fonctionnement d'un nouveau logiciel.

Le programme client de gestion de courrier électronique sécurisé assure plusieurs fonctions. Une fonction d'envoi de courrier chiffré comporte les opérations consistant à recevoir un message entré par l'utilisateur sur le dispositif d'interface 50, désigner un destinataire du message, sélectionner la clé publique de ce destinataire pour chiffrer le message et/ou signer le message avec la clé privée KR et envoyer le message chiffré et/ou signé au serveur 2b, comme indiqué par la flèche 66. Le message sera alors transmis via le réseau 1 au serveur de courrier électronique 62 du destinataire et le destinataire pourra consulter le message depuis son propre micro-ordinateur 64 équipée d'un programme client approprié. Une fonction de réception de courrier électronique chiffré comprend les opérations consistant à recevoir un message chiffré depuis le serveur 2b, comme indiqué par la flèche 68, déchiffrer le message avec la clé privée KR et/ou vérifier la signature du message avec la clé publique de l'expéditeur, et présenter le contenu du message à l'utilisateur.

En référence à la figure 6, on décrit un autre exemple de l'étape 46, dans lequel le service offert est un service de diffusion télévisée numérique. Le serveur 2c est un serveur de télévision numérique d'un fournisseur auprès duquel l'utilisateur est abonné. L'utilisateur utilise un dispositif d'interface 50 qui prend la forme d'un décodeur 70 pour télévision muni d'une télécommande 72.

A l'étape 46, l'application de session est exécutée par le décodeur 70 pour effectuer une authentification mutuelle entre l'utilisateur et le serveur 2c à l'aide du certificat A, comme il a été expliqué en référence à l'étape 22. Puis l'utilisateur sélectionne un programme télévisé au moyen de la télécommande 72. Le décodeur 70 transmet une requête de lecture correspondante 74 au serveur 2c. Après avoir vérifié que le programme télévisé demandé est autorisé par l'abonnement de l'utilisateur, le serveur 2c envoie au décodeur 70 un flux de données audio-vidéo correspondant 76, chiffré symétriquement

de manière à être déchiffré par le décodeur 70 au moyen de la clé KS ou d'une clé temporaire KT. Par exemple, la clé KS peut avoir été attribuée confidentiellement à l'utilisateur par le fournisseur lors des formalités d'abonnement ou avoir été transmise par le décodeur 70 au serveur 2c après l'authentification mutuelle.

Bien que l'invention ait été décrite en liaison avec plusieurs modes de réalisation particuliers, il est bien évident qu'elle n'y est nullement limitée et qu'elle comprend tous les équivalents techniques des moyens décrits ainsi que leurs combinaisons si celles-ci entrent dans le cadre de l'invention. En particulier, l'homme du métier remarquera que l'ordre d'exécution des étapes dans les modes de réalisations décrits peut être modifié selon de nombreuses variantes aboutissant essentiellement au même résultat et ne sortant pas du cadre de l'invention.

REVENDICATIONS

1. Procédé pour échanger de manière protégée des données de contenu en ligne, comportant les étapes consistant à :
recevoir (32) un code entré par un utilisateur dans un dispositif d'interface (4a-c , 50) relié à un premier dispositif serveur (3) par au moins un réseau de transport de données (1, 54),
envoyer (36) une requête de lecture depuis ledit dispositif d'interface audit premier dispositif serveur dans lequel sont stockées des données personnelles cryptographiques respectives d'une pluralité d'utilisateurs, lesdites données personnelles cryptographiques de chaque utilisateur étant chiffrées au moyen d'un code authentique respectif dudit utilisateur,
recevoir (42) les données personnelles cryptographiques chiffrées dudit utilisateur dans ledit dispositif d'interface,
déchiffrer (44) lesdites données personnelles cryptographiques au moyen dudit code entré lorsque ledit code entré correspond audit code authentique de l'utilisateur,
caractérisé par le fait qu'il comporte les étapes consistant à :
utiliser (46) lesdites données personnelles cryptographiques pour protéger un échange de données de contenu (58, 60, 66, 68, 76) entre ledit dispositif d'interface et au moins un deuxième dispositif serveur (2a-c) relié audit dispositif d'interface par au moins un réseau de transport de données,
supprimer (48) ledit code entré et lesdites données cryptographiques personnelles dudit dispositif d'interface.

2. Procédé selon la revendication 1, caractérisé par le fait que ledit dispositif d'interface et ledit premier dispositif serveur établissent un canal de communication confidentiel entre eux par mise en commun d'au moins une clé de chiffrement (Ks) présentant une grande entropie par rapport audit code authentique de l'utilisateur, lesdites données personnelles cryptographiques chiffrées ($F_{KP}(D_A)$) étant transmises audit dispositif d'interface par ledit canal de communication confidentiel.

3. Procédé selon la revendication 1 ou 2, caractérisé par le fait qu'au moins une donnée personnelle de vérification de code (VP) qui dérive dudit code authentique de l'utilisateur (P) selon une fonction

déterministe (h(N//.)) est stockée dans ledit premier dispositif serveur et que ledit premier dispositif serveur authentifie explicitement ou implicitement le dispositif d'interface à l'aide de ladite donnée personnelle de vérification de code.

4. Procédé selon la revendication 3, caractérisé par le fait que ladite fonction déterministe est une fonction non inversible résistante aux collisions.

5. Procédé selon la revendication 2 prise en combinaison avec la revendication 3 ou 4, caractérisé par le fait que ledit dispositif d'interface et ledit premier dispositif serveur réalisent simultanément la mise en commun de ladite au moins une clé de chiffrement et l'authentification explicite ou implicite dudit dispositif d'interface par ledit premier dispositif serveur en utilisant un protocole de type Password-Based-Key-Exchange (échange de clé basé sur un mot de passe) PBKE.

6. Procédé selon la revendication 5, caractérisé par le fait que ledit protocole de type Password-Based-Key-Exchange inclut une seule communication dans chaque sens entre ledit dispositif d'interface et ledit premier dispositif serveur, ladite communication depuis le premier dispositif serveur vers le dispositif d'interface incluant la transmission des données personnelles cryptographiques chiffrées.

7. Procédé selon l'une des revendications 4 à 6, caractérisé par le fait que ledit dispositif d'interface choisit un premier entier (a) correspondant à un premier élément (g^a mod p) d'un groupe prédéfini et ledit premier dispositif serveur choisit un deuxième entier (b) correspondant à un deuxième élément (g^b mod p) dudit groupe, puis ledit dispositif d'interface et ledit premier dispositif serveur se transmettent mutuellement lesdits premier et deuxième éléments, ledit dispositif d'interface et ledit premier dispositif serveur produisant chacun ladite au moins une clé de chiffrement (Ks) par combinaison de l'entier choisi par lui-même et de l'élément reçu par lui-même, ledit premier élément du groupe étant transmis audit premier dispositif serveur sous une forme chiffrée au moyen d'une trace discriminante (VP) qui dérive dudit code entré par l'utilisateur dans le dispositif d'interface selon ladite fonction déterministe, ledit premier élément du groupe étant déchiffré par ledit premier dispositif serveur au moyen de

ladite donnée personnelle de vérification de code (VP), ledit deuxième élément du groupe étant transmis audit dispositif d'interface sous une forme symétriquement chiffrée au moyen de ladite donnée personnelle de vérification de code, ledit deuxième élément du groupe étant déchiffré par ledit dispositif d'interface au moyen de ladite trace discriminante.

8. Procédé selon la revendication 7, caractérisé par le fait que lesdits premier et deuxième éléments du groupe sont chiffrés avec un protocole de chiffrement symétrique (E) qui est choisi de manière qu'une tentative de déchiffrement d'un desdits éléments du groupe selon ledit protocole produise toujours un élément dudit groupe, quelle que soit la donnée utilisée dans ladite tentative.

9. Procédé selon l'une des revendications 7 ou 8, caractérisé par le fait que lesdits premier et deuxième éléments du groupe sont chiffrés avec un protocole de chiffrement symétrique (E) qui est choisi de manière que ledit entier ne puisse pas être obtenu à partir de l'élément du groupe correspondant chiffré.

10. Procédé selon l'une des revendications 7 à 9, caractérisé par le fait que ledit premier élément du groupe, respectivement ledit deuxième élément du groupe, est chiffré avec un protocole de chiffrement symétrique (E) qui comprend l'étape consistant à composer ledit élément par une loi de composition dudit groupe avec l'image de ladite trace discriminante, respectivement l'image de ladite donnée personnelle de vérification de code, par une fonction à valeurs dans ledit groupe.

11. Procédé selon l'une des revendications 1 à 10, caractérisé par le fait que ladite étape d'utilisation comprend l'étape consistant à :
authentifier ledit utilisateur auprès dudit au moins un deuxième dispositif serveur au moyen de données d'authentification dudit utilisateur incluses dans lesdites données cryptographiques personnelles.

12. Procédé selon l'une des revendications 1 à 11, caractérisé par le fait que ladite étape d'utilisation comprend les étapes consistant à :
recevoir des données de contenu entrées par ledit utilisateur dans ledit dispositif d'interface,
chiffrer lesdites données de contenu au moyen d'au moins une clé de

chiffrement incluse dans lesdites données cryptographiques personnelles, envoyer lesdites données de contenu chiffrées (58, 66) audit au moins un deuxième dispositif serveur (2a-b) pour stocker lesdites données de contenu chiffrées dans ledit deuxième dispositif serveur et/ou les transmettre à un destinataire.

13. Procédé selon l'une des revendications 1 à 12, caractérisé par le fait que ladite étape d'utilisation comprend les étapes consistant à :
envoyer une deuxième requête de lecture désignant des données de contenu depuis ledit dispositif d'interface audit au moins un deuxième dispositif serveur (2a),
recevoir lesdites données de contenu chiffrées (60) depuis ledit au moins un deuxième dispositif serveur dans ledit dispositif d'interface,
déchiffrer lesdites données de contenu au moyen d'au moins une clé de déchiffrement incluse dans lesdites données personnelles cryptographiques.

14. Procédé selon l'une des revendications 1 à 13, caractérisé par le fait qu'il comporte l'étape consistant à :
imposer (38) un délai minimum prédéterminé entre le traitement de deux occurrences successives de ladite première requête de lecture au niveau du premier dispositif serveur, sous peine de ne pas tenir compte de l'occurrence la plus tardive.

15. Procédé selon l'une des revendications 1 à 14, caractérisé par le fait qu'il comporte une étape consistant à :
surveiller systématiquement (8) les communications impliquant ledit premier dispositif serveur (3).

16. Procédé selon l'une des revendications 1 à 15, caractérisé par le fait qu'il comporte l'étape consistant à :
contrôler l'intégrité des données personnelles cryptographiques reçues depuis ledit premier dispositif serveur au moyen de données de contrôle d'intégrité jointes auxdites données personnelles cryptographiques reçues depuis ledit premier dispositif serveur.

17. Procédé selon l'une des revendications 1 à 16, caractérisé par le fait qu'il comporte une étape d'inscription consistant à :
mettre à disposition (11, 12) des données personnelles cryptographiques

dans ledit dispositif d'interface,
recevoir (14) un code authentique entré par ledit utilisateur dans ledit dispositif d'interface,
chiffrer (20) lesdites données personnelles cryptographiques au moyen dudit code authentique,
envoyer (24) lesdites données personnelles cryptographiques chiffrées depuis ledit dispositif d'interface audit premier dispositif serveur pour stocker lesdites données personnelles cryptographiques chiffrées dans ledit premier dispositif serveur,
supprimer (28) lesdites données personnelles cryptographiques et ledit code authentique dudit dispositif d'interface.

18. Procédé selon la revendication 17, caractérisé par le fait que l'étape d'inscription comporte les étapes consistant à :
former (18) des données personnelles de vérification de code à partir dudit code authentique,
envoyer (24) lesdites données personnelles de vérification de code depuis ledit dispositif d'interface audit premier dispositif serveur pour stocker lesdites données personnelles de vérification de code dans ledit premier dispositif serveur.

19. Procédé selon la revendication 17 ou 18, caractérisé par le fait qu'il comporte une étape consistant à :
rejeter (14) ledit code authentique entré par l'utilisateur lorsque ledit code remplit des critères d'évidence prédéfinis.

20. Dispositif d'interface (4a-c, 50) pour échanger de manière protégée des données de contenu en ligne, comportant :
un moyen pour recevoir (32) un code entré par un utilisateur,
un moyen pour envoyer (36) une première requête de lecture depuis ledit dispositif d'interface à un premier dispositif serveur (3) dans lequel sont stockées des données personnelles cryptographiques respectives d'une pluralité d'utilisateurs, lesdites données personnelles cryptographiques de chaque utilisateur étant chiffrées au moyen d'un code authentique respectif dudit utilisateur,
un moyen pour recevoir (42) les données personnelles cryptographiques chiffrées dudit utilisateur,
un moyen pour déchiffrer (44) lesdites données personnelles cryptographiques au moyen dudit code entré lorsque ledit code entré

correspond audit code authentique de l'utilisateur,
caractérisé par :
des moyens pour utiliser (46) lesdites données personnelles cryptographiques afin de protéger un échange de données de contenu (58, 60, 66, 68, 76) entre ledit dispositif d'interface et au moins un deuxième dispositif serveur (2a-c),
un moyen pour supprimer (48) ledit code et lesdites données cryptographiques personnelles dudit dispositif d'interface.

21. Dispositif selon la revendication 20, caractérisé par le fait qu'il consiste en un programme de gestion de courrier électronique, lesdits moyens d'utilisation des données personnelles cryptographiques comprenant un module cryptographique pour signer, chiffrer et/ou déchiffrer des courriers électroniques à l'aide d'au moins certaines desdites données cryptographiques personnelles.

22. Dispositif selon la revendication 20, caractérisé par le fait qu'il consiste en un module d'extension adapté à un programme de gestion de courrier électronique comprenant un module cryptographique pour signer, chiffrer et déchiffrer des courriers électroniques, lesdits moyens d'utilisation des données personnelles cryptographiques comprenant un moyen pour fournir audit module cryptographique au moins certaines desdites données cryptographiques personnelles.

23. Dispositif d'interface d'inscription (4a-c, 50), caractérisé par le fait qu'il comporte :
un moyen pour mettre à disposition (11, 12) des données personnelles cryptographiques dans ledit dispositif d'interface,
un moyen (6) pour recevoir (14) un code authentique entré par ledit utilisateur dans ledit dispositif d'interface,
un moyen pour chiffrer (20) lesdites données personnelles cryptographiques au moyen dudit code authentique,
un moyen pour envoyer (24) lesdites données personnelles cryptographiques chiffrées depuis ledit dispositif d'interface à un premier dispositif serveur (3) pour stocker lesdites données personnelles cryptographiques chiffrées dans ledit premier dispositif serveur, dans lequel sont stockées des données personnelles cryptographiques respectives d'une pluralité d'utilisateurs, lesdites données personnelles cryptographiques de chaque utilisateur étant chiffrées au moyen d'un

code authentique respectif dudit utilisateur,
un moyen pour supprimer (28) lesdites données personnelles cryptographiques et ledit code authentique dudit dispositif d'interface.

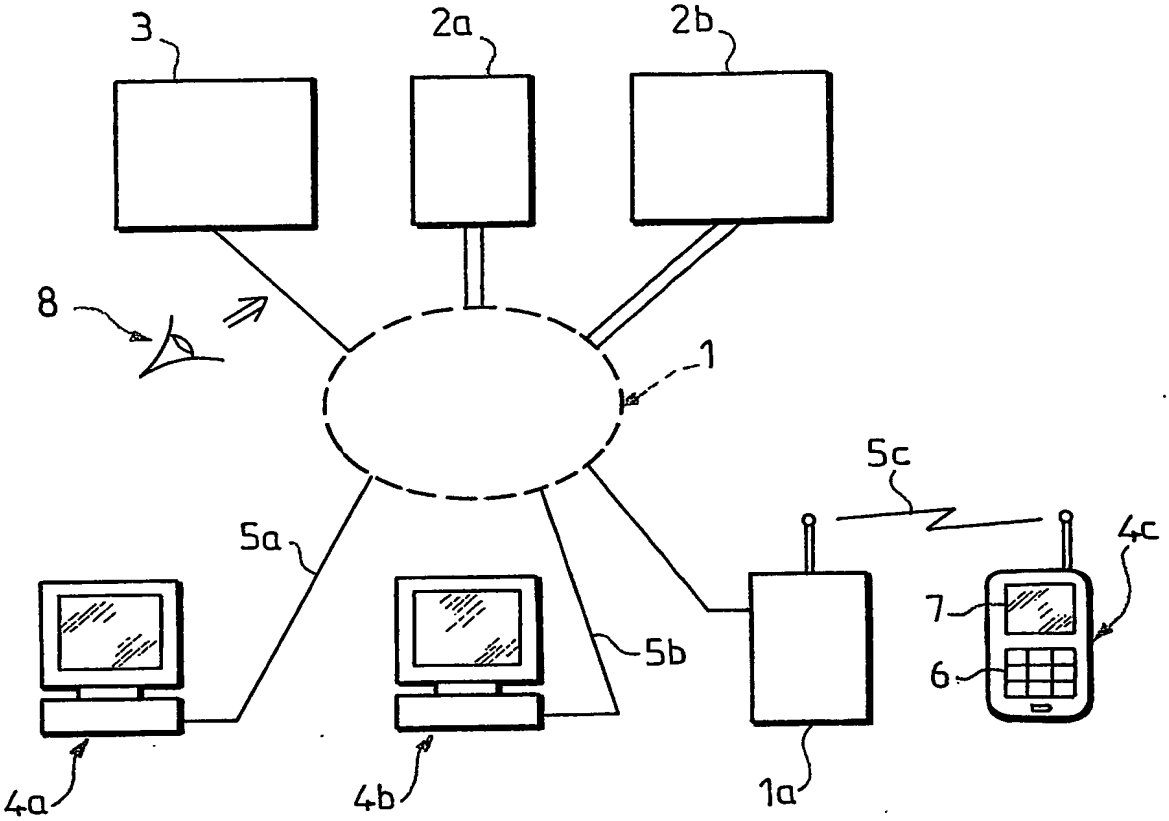


FIG.1

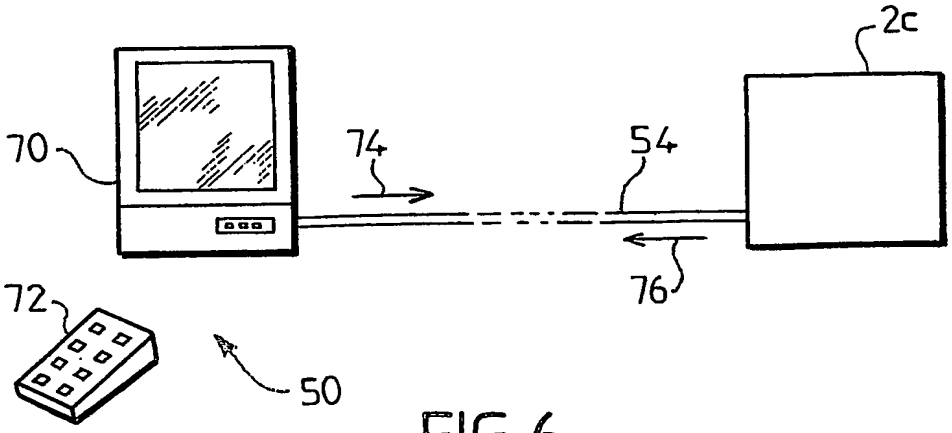


FIG.6

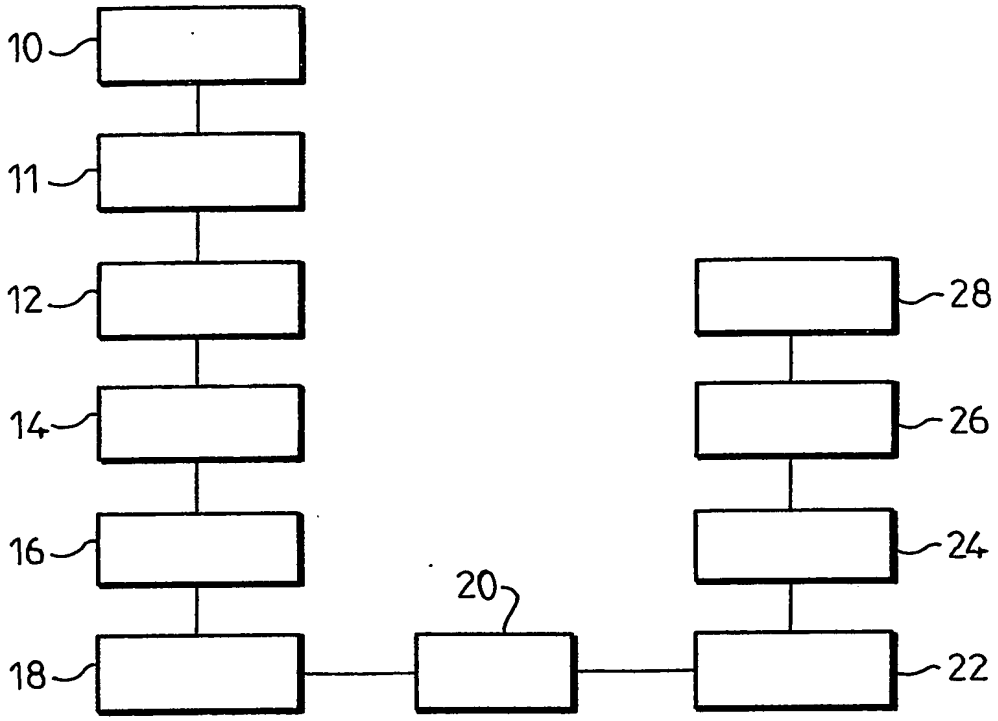


FIG. 2

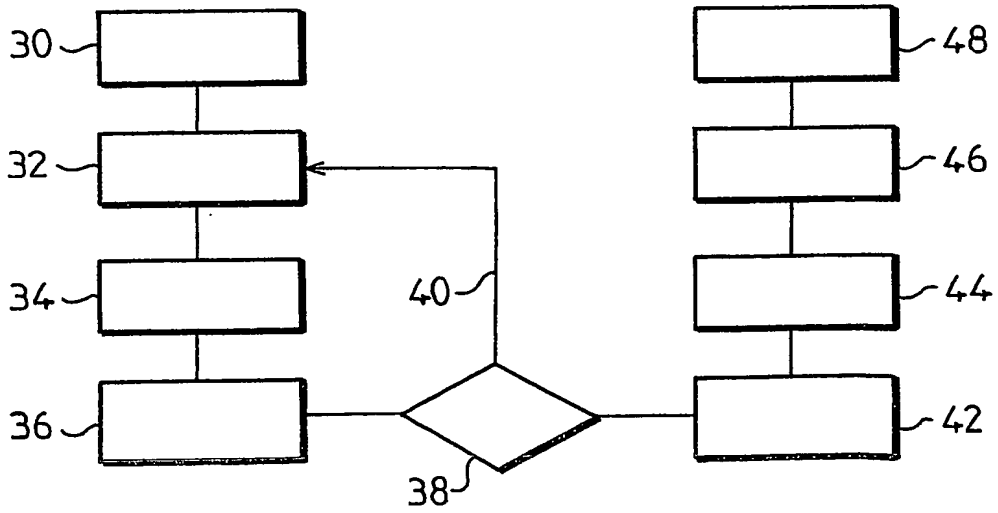


FIG. 3

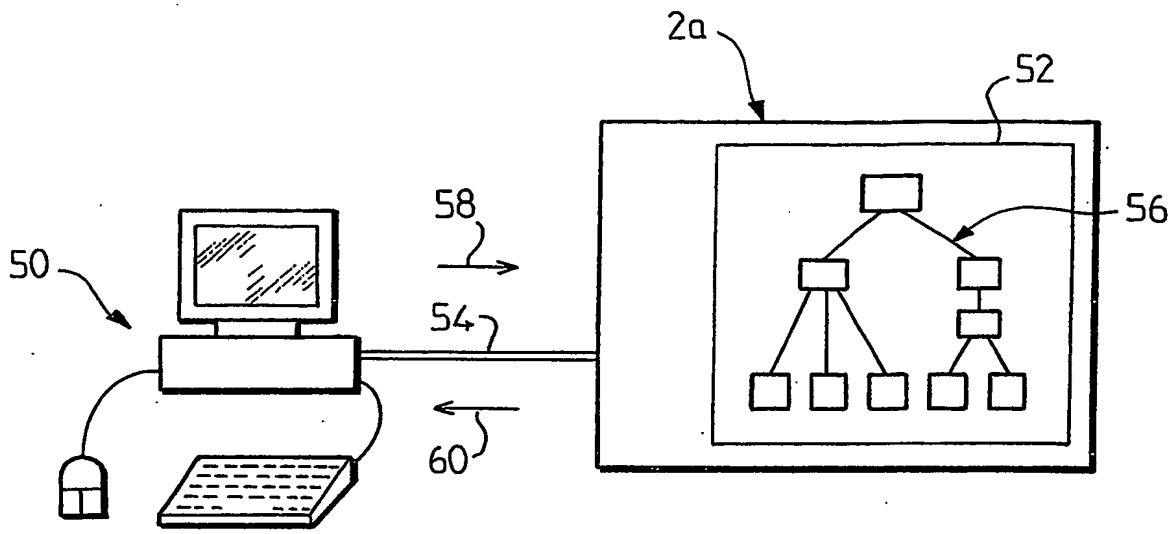


FIG.4

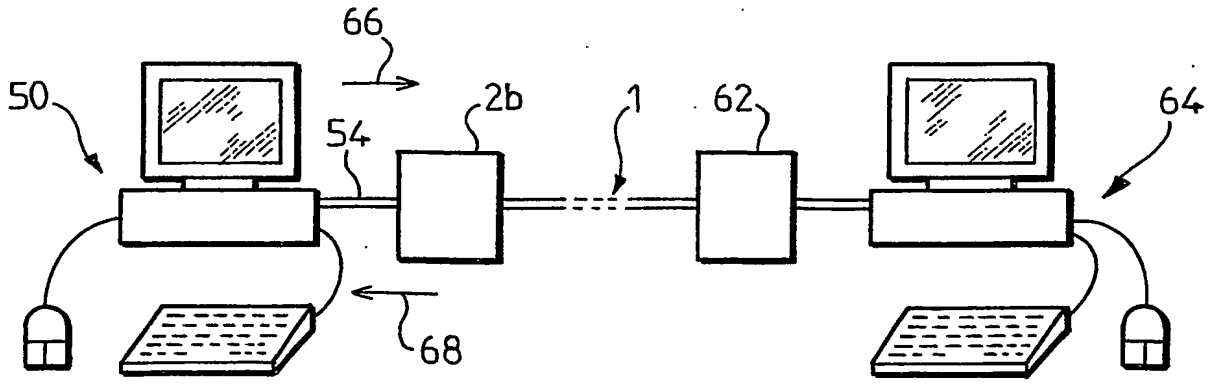


FIG.5

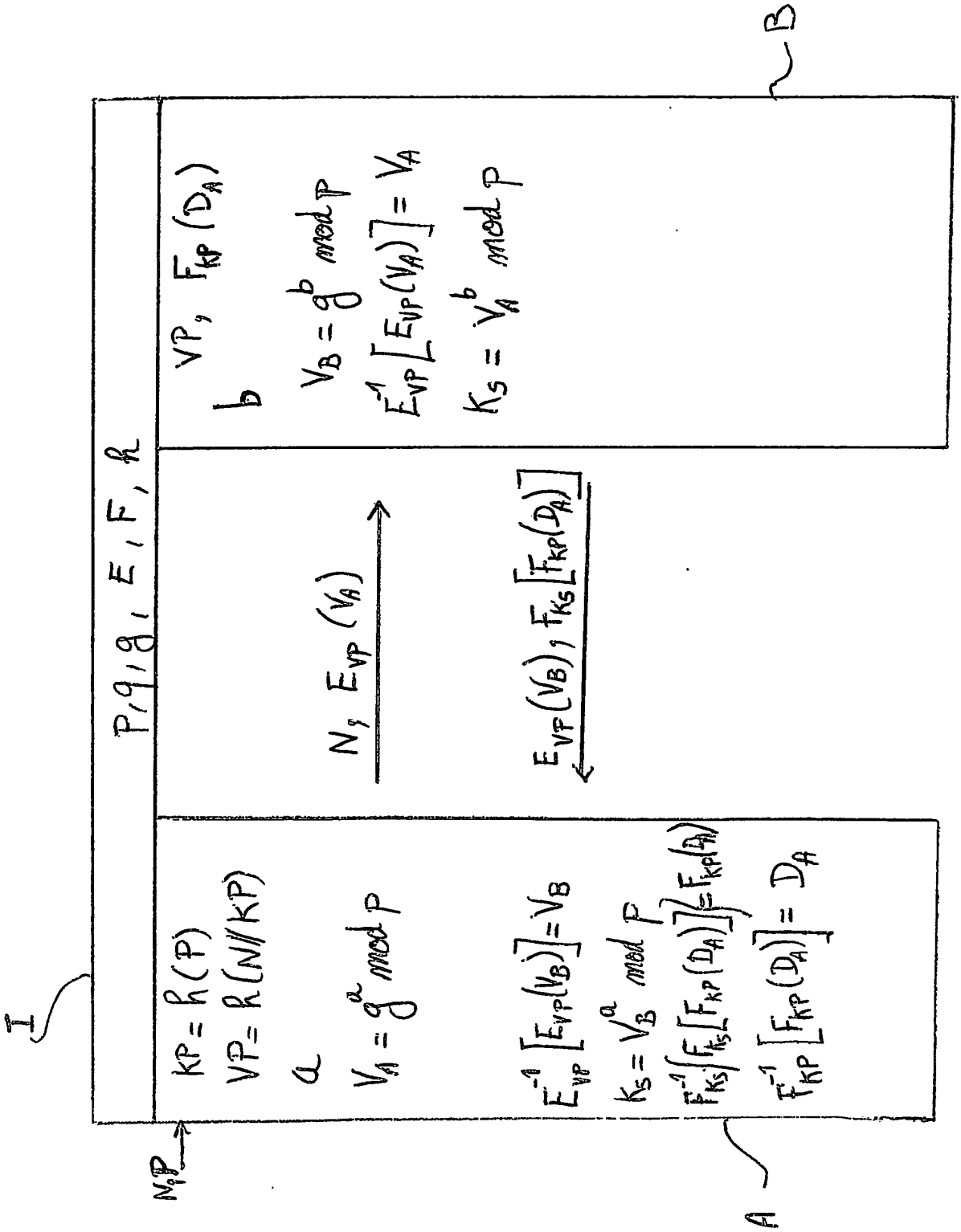

I
P, q, g, E, F, R
KP = R(P)
VP = R(N // KP)
a
$V_A = g^a \bmod P$
$E_{VP}^{-1}[E_{VP}(V_B)] = V_B$
$K_S = V_B^a \bmod P$
$F_{KS}^{-1}[F_{KS}[F_{KP}(D_A)]] = F_{KP}(D_A)$
$F_{KP}^{-1}[F_{KP}(D_A)] = D_A$
A
N, P
$N, E_{VP}(V_A)$
$E_{VP}(V_B), F_{KS}[F_{KP}(D_A)]$
B
b
VP, $F_{KP}(D_A)$
$V_B = g^b \bmod P$
$E_{VP}^{-1}[E_{VP}(V_A)] = V_A$
$K_S = V_A^b \bmod P$

FIG. 7

INTERNATIONAL SEARCH REPORT

International Application No
PCT/[redacted]3/01841

A. CLASSIFICATION OF SUBJECT MAT[redacted]
IPC 7 H04L9/32 H04L9/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5 491 752 A (KAUFMAN CHARLES W ET AL) 13 February 1996 (1996-02-13) cited in the application column 4, line 4 - line 20; figure 3	1,20,23
Y	US 2002/029340 A1 (CRISTY JOHN J ET AL) 7 March 2002 (2002-03-07) abstract paragraph '0007! paragraph '0017! paragraph '0021! paragraph '0024! paragraph '0043! paragraph '0050!	1,20,23
A	US 2001/034841 A1 (SHAMBROOM W DAVID) 25 October 2001 (2001-10-25) paragraph '0061! - paragraph '0062!	1,20,23

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
6 November 2003	17/11/2003

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Holper, G

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSID[redacted] TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	BELLOVIN S M ET AL: "ENCRYPTED KEY EXCHANGE: PASSWORD-BASED PROTOCOLS SECURE AGAINST DICTIONARY ATTACKS" PROCEEDINGS OF THE COMPUTER SOCIETY SYMPOSIUM ON RESEARCH IN SECURITY AND PRIVACY. OAKLAND, MAY 4 - 6, 1992, LOS ALAMITOS, IEEE COMP. SOC. PRESS, US, vol. SYMP. 13, 4 May 1992 (1992-05-04), pages 72-84, XP000326480 ISBN: 0-8186-2825-1 cited in the application page 78, right-hand column, line 27 -page 79, right-hand column, line 6 ---	2,5-7
A	US 6 230 269 B1 (MISRA PRADYUMNA K ET AL) 8 May 2001 (2001-05-08) abstract column 5, line 31 -column 6, last line column 7, line 48 - line 59 ---	3
A	EP 0 535 863 A (AMERICAN TELEPHONE & TELEGRAPH) 7 April 1993 (1993-04-07) figure 5 ---	2,5-7
A	US 6 230 272 B1 (LOCKHART ROLAND T ET AL) 8 May 2001 (2001-05-08) column 1, line 32 - line 54 column 4, line 8 - line 13 column 5, line 33 - line 65 column 6, line 4 - line 63; figure 3 ---	1,20,23
A	EP 1 059 761 A (INTERNAT COMPUTERS LTD) 13 December 2000 (2000-12-13) column 5, line 22 - line 32; figure 2 -----	1,20,23

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
US 5491752	A	13-02-1996	US	5373559 A	13-12-1994
US 2002029340	A1	07-03-2002	US	2001052074 A1	13-12-2001
			US	6289450 B1	11-09-2001
			AU	5280400 A	18-12-2000
			WO	0074299 A1	07-12-2000
US 2001034841	A1	25-10-2001	US	6198824 B1	06-03-2001
			US	5923756 A	13-07-1999
			US	2001020274 A1	06-09-2001
			EP	0960500 A1	01-12-1999
			JP	2001511982 T	14-08-2001
			WO	9836522 A1	20-08-1998
			US	6301661 B1	09-10-2001
US 6230269	B1	08-05-2001	NONE		
EP 0535863	A	07-04-1993	US	5241599 A	31-08-1993
			AU	648433 B2	21-04-1994
			AU	2351392 A	08-04-1993
			CA	2076252 A1	03-04-1993
			DE	69232369 D1	14-03-2002
			DE	69232369 T2	23-01-2003
			EP	1104959 A2	06-06-2001
			EP	0535863 A2	07-04-1993
			JP	2599871 B2	16-04-1997
			JP	6169306 A	14-06-1994
			NO	923740 A	05-04-1993
US 6230272	B1	08-05-2001	NONE		
EP 1059761	A	13-12-2000	GB	2350981 A	13-12-2000
			DE	60001290 D1	06-03-2003
			EP	1059761 A1	13-12-2000

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/[redacted]03/01841

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L9/32 H04L9/08

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y	US 5 491 752 A (KAUFMAN CHARLES W ET AL) 13 février 1996 (1996-02-13) cité dans la demande colonne 4, ligne 4 - ligne 20; figure 3	1,20,23
Y	US 2002/029340 A1 (CRISTY JOHN J ET AL) 7 mars 2002 (2002-03-07) abrégé alinéa '0007! alinéa '0017! alinéa '0021! alinéa '0024! alinéa '0043! alinéa '0050!	1,20,23
A	US 2001/034841 A1 (SHAMBROOM W DAVID) 25 octobre 2001 (2001-10-25) alinéa '0061! - alinéa '0062!	1,20,23

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
6 novembre 2003	17/11/2003

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Holper, G

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

C.(suite) DOCUMENTS CONSIDERES C[redacted] PERTINENTS

Catégorie °	Identification des documents cités, avec,le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
A	BELLOVIN S M ET AL: "ENCRYPTED KEY EXCHANGE: PASSWORD-BASED PROTOCOLS SECURE AGAINST DICTIONARY ATTACKS" PROCEEDINGS OF THE COMPUTER SOCIETY SYMPOSIUM ON RESEARCH IN SECURITY AND PRIVACY. OAKLAND, MAY 4 - 6, 1992, LOS ALAMITOS, IEEE COMP. SOC. PRESS, US, vol. SYMP. 13, 4 mai 1992 (1992-05-04), pages 72-84, XP000326480 ISBN: 0-8186-2825-1 cité dans la demande page 78, colonne de droite, ligne 27 -page 79, colonne de droite, ligne 6	2,5-7
A	US 6 230 269 B1 (MISRA PRADYUMNA K ET AL) 8 mai 2001 (2001-05-08) abrégé colonne 5, ligne 31 -colonne 6, dernière ligne colonne 7, ligne 48 - ligne 59	3
A	EP 0 535 863 A (AMERICAN TELEPHONE & TELEGRAPH) 7 avril 1993 (1993-04-07) figure 5	2,5-7
A	US 6 230 272 B1 (LOCKHART ROLAND T ET AL) 8 mai 2001 (2001-05-08) colonne 1, ligne 32 - ligne 54 colonne 4, ligne 8 - ligne 13 colonne 5, ligne 33 - ligne 65 colonne 6, ligne 4 - ligne 63; figure 3	1,20,23
A	EP 1 059 761 A (INTERNAT COMPUTERS LTD) 13 décembre 2000 (2000-12-13) colonne 5, ligne 22 - ligne 32; figure 2	1,20,23

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
US 5491752	A	13-02-1996	US	5373559 A	13-12-1994
US 2002029340	A1	07-03-2002	US	2001052074 A1	13-12-2001
			US	6289450 B1	11-09-2001
			AU	5280400 A	18-12-2000
			WO	0074299 A1	07-12-2000
US 2001034841	A1	25-10-2001	US	6198824 B1	06-03-2001
			US	5923756 A	13-07-1999
			US	2001020274 A1	06-09-2001
			EP	0960500 A1	01-12-1999
			JP	2001511982 T	14-08-2001
			WO	9836522 A1	20-08-1998
			US	6301661 B1	09-10-2001
US 6230269	B1	08-05-2001	AUCUN		
EP 0535863	A	07-04-1993	US	5241599 A	31-08-1993
			AU	648433 B2	21-04-1994
			AU	2351392 A	08-04-1993
			CA	2076252 A1	03-04-1993
			DE	69232369 D1	14-03-2002
			DE	69232369 T2	23-01-2003
			EP	1104959 A2	06-06-2001
			EP	0535863 A2	07-04-1993
			JP	2599871 B2	16-04-1997
			JP	6169306 A	14-06-1994
			NO	923740 A	05-04-1993
US 6230272	B1	08-05-2001	AUCUN		
EP 1059761	A	13-12-2000	GB	2350981 A	13-12-2000
			DE	60001290 D1	06-03-2003
			EP	1059761 A1	13-12-2000

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.